SOPHOS

SafeGuard® Enterprise 5.50

manuel d'installation

Date du document : Novembre 2010

Table des matières

1 Présentation de SafeGuard Enterprise 3

2 Composants de SafeGuard Enterprise 4

3 Préparation pour l'installation 6

4 Configuration de la base de données SafeGuard Enterprise 17

5 Configuration de SafeGuard Management Center 27

6 Configuration du serveur SafeGuard Enterprise 43

7 Test de la communication 56

8 Réplication de la base de données SafeGuard Enterprise 61

9 Configuration d'une structure organisationnelle 67

10 Configurations de SafeGuard pour les ordinateurs finaux 72

11 Installation centralisée des ordinateurs finaux 80

12 Configuration locale des ordinateurs finaux 97

13 Installation du logiciel client SafeGuard Enterprise sur les ordinateurs disposant de plusieurs systèmes d'exploitation 101

14 Installation de SafeGuard Configuration Protection 104

15 Empêchement de la désinstallation sur le PC de l'utilisateur 109

16 Mise à jour de SafeGuard Enterprise 110

17 Mise à niveau de Sophos SafeGuard 5.5x vers SafeGuard Enterprise 117

18 Mise à niveau de SafeGuard Easy 4.x/Sophos SafeGuard Disk Encryption 4.x vers SafeGuard Enterprise 119

19 Mise à jour du système d'exploitation 128

20 Annexe : Scénario de pratique recommandée 129

21 Support technique 130

22 Copyright 131

1 Présentation de SafeGuard Enterprise

SafeGuard Enterprise est une solution de sécurité des données complète et modulaire, qui utilise une stratégie de chiffrement basé sur une règle pour protéger les informations et les partager sur les serveurs, les PC et les périphériques terminaux mobiles.

L'administration centralisée est effectuée par SafeGuard Enterprise Management Center. Les stratégies de sécurité, les clés, les certificats, les cartes à puce et les clés cryptographiques peuvent être gérés à l'aide d'une stratégie d'administration basée sur les rôles clairement définie. Les journaux détaillés et les rapports garantissent aux utilisateurs et aux administrateurs de toujours être informés de l'ensemble des événements.

Du côté des utilisateurs, le chiffrement des données et leur protection contre tout accès non autorisé constituent les principales fonctions de sécurité de SafeGuard Enterprise. SafeGuard Enterprise peut être intégré de façon transparente à l'environnement normal de l'utilisateur, et son utilisation est facile et intuitive. Le propre système d'authentification de SafeGuard, l'authentification au démarrage (POA, Power-On Authentication), fournit la nécessaire protection des accès et offre une prise en charge conviviale lors de la récupération des informations d'identification.

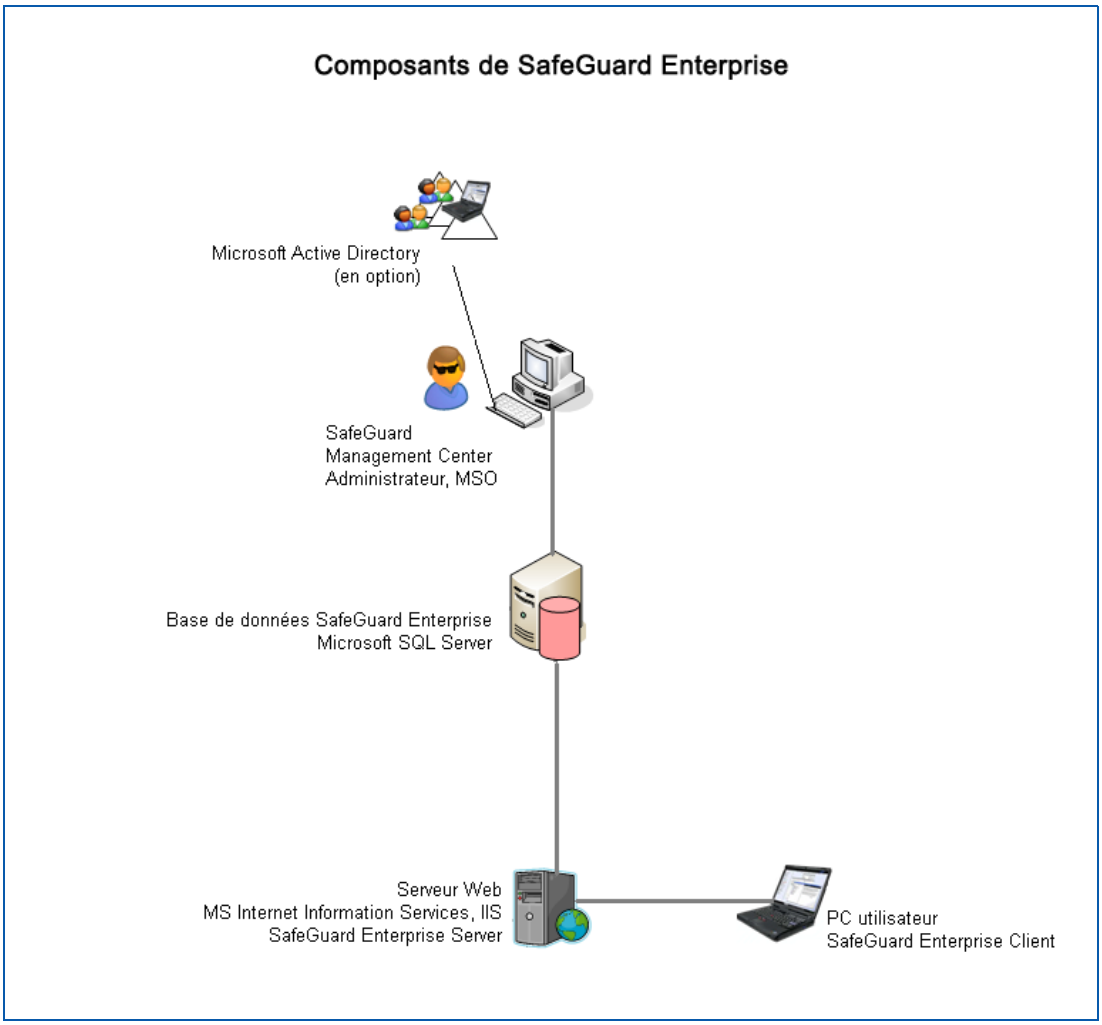
CONSEIL : Nos didacticiels vidéo constituent le moyen idéal pour découvrir SafeGuard Enterprise. Ils figurent sur le CD du produit dans la rubrique Didacticiels. Ils décrivent l'installation de SafeGuard Enterprise et l'utilisation de SafeGuard Management Center.

2 Composants de SafeGuard Enterprise

Dans ce chapitre, vous prendrez connaissance des composants de SafeGuard Enterprise et apprendrez comment les composants individuels fonctionnent les uns avec les autres.

Une ou plusieurs bases de données Microsoft SQL stockent les informations relatives aux ordinateurs finaux sur le réseau d'entreprise. L'administrateur, appelé dans SafeGuard Enterprise responsable principal de la sécurité (MSO, Master Security Officer), utilise SafeGuard Management Center pour gérer le contenu de la base de données et créer des instructions de sécurité (stratégies).

Les PC/ordinateurs portatifs d'utilisateur lisent les stratégies dans la base de données et signalent à celle-ci leur exécution correcte. La communication entre la base de données et les ordinateurs finaux est établie par le serveur Web IIS (Internet Information Services) sur lequel le serveur SafeGuard Enterprise est installé.



Le tableau suivant décrit les composants individuels :

Composant	Description
Bases de données SafeGuard Enterprise basées sur la base de données Microsoft SQL Server	Les bases de données SafeGuard Enterprise contiennent toutes les données pertinentes, telles que les clés/certificats, les informations sur les utilisateurs et les ordinateurs, les événements et les paramètres de stratégie. Elles doivent être accessibles au serveur SafeGuard Enterprise et à un seul responsable de la sécurité de SafeGuard Management Center, habituellement le MSO. Les bases de données SafeGuard Enterprise peuvent être générées et configurées à l'aide d'un assistant ou de scripts.
Serveur SafeGuard Enterprise sur serveur Web IIS	**Microsoft Internet Information Services (ISS) avec .NET Framework 3.0 SP 1 et ASP.NET 2.0** Le serveur Web utilisé pour SafeGuard Enterprise doit être basé sur IIS. Nous recommandons d'utiliser un serveur IIS dédié pour le serveur SafeGuard Enterprise. Le serveur IIS peut être mis en cluster.
	Serveur SafeGuard Enterprise Interface entre la base de données et les ordinateurs finaux SafeGuard Enterprise. Sur demande, le serveur SafeGuard Enterprise envoie les paramètres de stratégie aux ordinateurs finaux. Il doit pouvoir accéder à la base de données. Il s'exécute en tant qu'application sur un serveur Web IIS.
SafeGuard Management Center avec .NET Framework 3.0 SP 1 et ASP.Net 2.0 sur PC d'administrateur	Outil de gestion centralisée de SafeGuard Enterprise permettant de gérer les clés et les certificats, les utilisateurs et les ordinateurs, et de créer des stratégies SafeGuard Enterprise. SafeGuard Management Center communique avec la base de données.
Services d'annuaire (facultatif)	Importation d'un annuaire actif, qui contient la structure organisationnelle de l'entreprise avec les utilisateurs et les ordinateurs.
Client SafeGuard Enterprise sur des ordinateurs finaux	Logiciel client pour l'authentification et le chiffrement des données sur les ordinateurs finaux. Le client SafeGuard Enterprise communique avec le serveur SafeGuard Enterprise.

3 Préparation pour l'installation

Ce chapitre décrit comment préparer l'installation de SafeGuard Enterprise.

3.1 Premières étapes préalables à l'installation

Quelques préparations sont nécessaires à l'installation. Nous vous invitons à lire attentivement la liste suivante et à vérifier que vous répondez à l'ensemble des points définis.

Préparation générale

- Fermez toutes les applications ouvertes.
- Vous devez disposer des droits d'administrateur Windows.
- Vérifiez que l'espace disque disponible est suffisant. Les informations afférentes se trouvent dans les notes de version.
- Veuillez les lire avec attention.

Préparations pour le chiffrement

- Un compte utilisateur doit être configuré et actif sur l'ordinateur final.
- La sauvegarde complète des données doit être exécutée sur l'ordinateur final.
- Vous devez rechercher la présence d'éventuelles erreurs sur le ou les disques durs à l'aide de cette commande `chkdsk` :

  chkdsk %systemdrive% /F /V /L /X

  Dans certains cas, vous serez peut-être invité à redémarrer l'ordinateur et à réexécuter la commande chkdsk.

  Vous trouverez plus d'informations sur ce sujet dans la base de connaissances (en anglais) :

  http://www.sophos.com/support/knowledgebase/article/107799.html.
- Utilisez l'outil « defrag » intégré à Windows pour repérer et consolider les fichiers d'initialisation, fichiers de données et dossiers fragmentés sur les volumes locaux. Vous trouverez plus d'informations sur ce sujet dans la base de connaissances (en anglais) : *http://www.sophos.com/support/knowledgebase/article/109226.html*.
- Désinstallez les gestionnaires d'amorçage tiers tels que « PROnetworks Boot Pro » et « Boot-US ».
- Si vous avez utilisé un outil d'imagerie/de clonage, nous recommandons la réécriture du MBR. Pour installer SafeGuard Enterprise, vous avez besoin d'un enregistrement de démarrage principal « impeccable ». Il se peut que l'utilisation de programmes d'imagerie/de clonage ait affecté l'état de cet enregistrement.

Vous pouvez nettoyer l'enregistrement de démarrage principal en procédant à un amorçage depuis un CD Windows et en utilisant la commande FIXMBR à partir de la Console de récupération Windows.

Pour plus d'informations, consultez la base de connaissances (en anglais) : *http://www.sophos.com/support/knowledgebase/article/108088.html*.

- Si la partition d'amorçage a été convertie du format FAT au format NTFS et que le système n'a pas été redémarré, vous ne devez pas installer SafeGuard Enterprise. L'installation peut ne pas se terminer correctement, car le système de fichiers était encore FAT au moment de l'installation tandis que le format NTFS a été trouvé au moment de l'activation. Dans ce cas, vous devriez réinitialiser l'ordinateur une fois avant l'installation de SafeGuard Enterprise.

De nouvelles fonctionnalités sont régulièrement ajoutées à SafeGuard Enterprise, car il s'agit d'un logiciel pouvant être mis à niveau. Il se peut donc que votre version fournisse des fonctionnalités que nous n'avons pas pu insérer dans le manuel ou dans l'aide en ligne avant le délai éditorial. Ces modifications sont décrites dans les notes de version. Vous devez donc les lire avec attention avant l'installation.

3.2 Configuration minimale du système

Reportez-vous aux notes de version pour connaître les détails relatifs à la configuration requise pour le matériel et le logiciel, les service packs et l'espace disque requis lors de l'installation et pour garantir un bon fonctionnement.

Exigences spécifiques pour les ordinateurs finaux :

AHCI

Si Intel AHCI (Advanced Host Controller Interface) est utilisé sur l'ordinateur, le disque dur d'amorçage doit être installé dans le slot 0 ou le slot 1. Vous pouvez insérer jusqu'à 32 disques durs. SafeGuard Enterprise ne fonctionne que sur les deux premiers numéros de slot.

Disques dynamiques et GPT

Les disques dynamiques et GPT (GUID Partition Table) ne sont pas pris en charge. Dans ces cas-là, l'installation est interrompue. Si de tels disques sont trouvés sur l'ordinateur ultérieurement, ils ne sont pas pris en charge.

Disques durs SCSI

Le client SafeGuard Enterprise Device Encryption ne prend pas en charge les systèmes équipés de disques durs reliés par un bus SCSI.

3.3 Packages d'installation

Les CD du produit contiennent les composants du programme d'installation de SafeGuard Enterprise sous la forme de packages .msi.

Avis : Si vous utilisez le système d'exploitation Windows 7 64 bits ou Windows Vista 64 bits sur les ordinateurs finaux (<nom package>_x64.msi), vous pourrez installer la variante 64 bits des packages « client » .msi. Le package 64 bits de SafeGuard Configuration Protection est disponible pour Windows 7 64 bits.

Les packages .msi suivants sont fournis :

Package d'installation	Description
SGNServer.msi	Serveur SafeGuard Enterprise
SGNManagementCenter.msi	SafeGuard Management Center pour l'administration centralisée des domaines, des clés, des stratégies, etc.
SGxClientPreinstall.msi	Doit être installé sur les ordinateurs finaux avant le logiciel de chiffrement (obligatoire). Fournit aux ordinateurs finaux la configuration requise pour une installation réussie du logiciel de chiffrement.
SGNClient.msi SGNClient_x64.msi	Chiffrement basé sur volume et sur fichier avec SafeGuard Data Exchange, pour les clients SafeGuard Enterprise (gérés) et les clients Sophos SafeGuard (autonomes).
SGNClient_withoutDE.msi SGNClient_withoutDE_x64.msi	SafeGuard Data Exchange avec un chiffrement basé sur fichier sans authentification au démarrage, pour les clients SafeGuard Enterprise (gérés) et les clients Sophos SafeGuard (autonomes).
SGN_CP_Client.msi SGN_CP_Client_x64.msi (disponible pour Windows 7 64 bits)	SafeGuard Configuration Protection : protection des ports et gestion des périphériques sur les ordinateurs finaux. SafeGuard Configuration Protection n'est PAS disponible pour les clients Sophos SafeGuard (autonomes). Le package 64 bits de SafeGuard Configuration Protection est disponible pour Windows 7 64 bits.
SGNClientRuntime.msi SGNClientRuntime_x64.msi	Client d'exécution qui permet l'initialisation à partir d'un volume d'initialisation secondaire lorsque plusieurs systèmes d'exploitation sont installés et qui accède à ces volumes lorsqu'ils sont chiffrés par une installation de SafeGuard Enterprise sur le volume primaire. Disponible pour les clients SafeGuard Enterprise (gérés) et les clients Sophos SafeGuard (autonomes).

De plus, les packages de configuration doivent être générés pendant l'installation.

3.4 Langue de l'interface utilisateur

Définissez la langue de SafeGuard Enterprise sur le client, dans Management Center en utilisant le type de stratégie **Paramètres généraux** > **Personnalisation** > **Langue du client** :

- La langue du produit SafeGuard Enterprise est identique à la langue du système d'exploitation, si celle-ci est définie. Si la langue du système d'exploitation appropriée n'est pas disponible dans SafeGuard Enterprise, la langue de SafeGuard Enterprise est définie par défaut sur l'anglais.
- Si l'une des langues disponibles est sélectionnée, les composants du produit SafeGuard Enterprise, côté client, s'affichent dans la langue sélectionnée.

Définissez la langue de SafeGuard Management Center dans Management Center :

- Ouvrez le menu **Outils** > **Options** > **Général** > **Langue de SafeGuard Management Center**, puis sélectionnez une langue.
- Redémarrez SafeGuard Management Center, qui s'affiche alors dans la langue sélectionnée.

Configuration de la langue

Les langues des assistants d'installation et de configuration correspondent automatiquement aux préférences de langue du système d'exploitation de l'ordinateur. L'anglais, l'allemand, le français et le japonais sont pris en charge pour les assistants d'installation et de configuration. Par exemple, si la langue du système d'exploitation est l'anglais, la langue de l'assistant d'installation sera également l'anglais.

3.5 Interaction avec les autres produits SafeGuard

3.5.1 Interaction avec SafeGuard LAN Crypt

Notez les éléments suivants :

- SafeGuard LAN Crypt 3.7x et SafeGuard Enterprise 5.50 peuvent coexister sur le même ordinateur et sont entièrement compatibles.
- SafeGuard LAN Crypt de version antérieure à la version 3.7x et SafeGuard Enterprise 5.5x ne peuvent pas coexister sur un même ordinateur.
  Si vous essayez d'installer SafeGuard Enterprise 5.50 sur un ordinateur où SafeGuard LAN Crypt 3.6x ou version antérieure est déjà installé, l'installation est annulée et un message d'erreur s'affiche.
- SafeGuard LAN Crypt 3.7x et SafeGuard Enterprise de version antérieure à la version 5.35.4 ne peuvent pas coexister sur un même ordinateur.
  Si vous essayez d'installer SafeGuard LAN Crypt 3.7x sur un ordinateur où SafeGuard Enterprise de version antérieure à la version 5.35.4 est déjà installé, l'installation est annulée et un message d'erreur s'affiche.

3.5.2 Interaction avec SafeGuard PrivateCrypto et SafeGuard PrivateDisk

SafeGuard Enterprise 5.5x et les produits autonomes SafeGuard PrivateCrypto et SafeGuard PrivateDisk à partir de la version 2.30 peuvent coexister sur le même ordinateur.

- SafeGuard PrivateCrypto et SafeGuard PrivateDisk peuvent alors partager la gestion des clés avec SafeGuard Enterprise.

3.5.3 Interaction avec SafeGuard Removable Media

Les modules SafeGuard Data Exchange et SafeGuard Removable Media ne peuvent pas coexister sur le même ordinateur. Avant d'installer le module SafeGuard Data Exchange sur un ordinateur final, vérifiez si SafeGuard Removable Media est déjà installé. Si tel est le cas, vous devez désinstaller SafeGuard Removable Media avant d'installer SafeGuard Data Exchange sur l'ordinateur final.

3.6 Protection des connexions de transport avec SSL

Pour renforcer la sécurité, SafeGuard Enterprise prend en charge le chiffrement des connexions de transport avec SSL entre ses composants :

- La connexion entre le serveur de base de données et le serveur Web ainsi que la connexion entre le serveur de base de données et l'ordinateur sur lequel se trouve SafeGuard Management Center peuvent être chiffrées avec SSL.

  SafeGuard Enterprise prend en charge la configuration d'une connexion à la base de données spécifique pour tout serveur Web enregistré.

- La connexion entre le serveur SafeGuard Enterprise et le client SafeGuard Enterprise peut être protégée via SSL ou un chiffrement exclusif SafeGuard. Le protocole SSL présente l'avantage d'être standard et de permettre d'établir une connexion plus rapidement qu'en utilisant le chiffrement de transport SafeGuard.

Le chiffrement SSL pour SafeGuard Enterprise peut être défini lors de la configuration des composants de SafeGuard Enterprise directement après l'installation. Il est également possible de l'activer ultérieurement et à tout moment. Les composants ne doivent pas être réinstallés si SSL est activé ultérieurement. Un nouveau package de configuration peut tout au plus être créé et déployé sur le serveur ou le client concerné.

Cependant, avant d'activer SSL dans SafeGuard Enterprise, il est nécessaire de configurer un environnement SSL.

AVIS :
Mesures de sécurité générales :
les ordinateurs sur lesquels le serveur SafeGuard Enterprise, la base de données et Management Center sont exécutés, doivent être protégés contre les attaques locales non autorisées. Voici quelques mesures pratiques qui peuvent être prises :

- Faites uniquement appel à des administrateurs de confiance ou appliquez la règle dite des deux personnes.
- Protégez-vous contre les attaques électroniques (pare-feu, configuration sécurisée, analyse de virus, mises à jour régulières, mots de passe renforcés, etc.).
- Protégez-vous contre les accès physiques (par exemple avec des salles sécurisées).

3.6.1 Configuration de SSL

Avant d'activer le chiffrement SSL dans SafeGuard Enterprise, vous devez configurer votre serveur Web, serveur de base de données et ordinateurs finaux.

Les tâches générales suivantes sont nécessaires pour configurer le serveur Web avec SSL :

- Un certificat doit être généré et le serveur IIS configuré pour utiliser SSL et sélectionner le certificat.
- Le nom du serveur spécifié lors de la configuration du serveur SafeGuard Enterprise doit être identique à celui spécifié dans le certificat SSL. Sinon, le client et le serveur ne peuvent pas communiquer. Un certificat distinct est nécessaire pour chaque serveur SafeGuard Enterprise.
- Si vous utilisez un équilibreur de charge réseau, vérifiez que la plage de ports inclut le port SSL.

Pour plus d'informations sur la configuration de SSL, consultez les liens suivants ou contactez le support technique (en anglais) :

http://msdn2.microsoft.com/en-us/library/ms998300.aspx

http://support.microsoft.com/default.aspx?scid=kb;en-us;316898

https://blogs.msdn.com/sql_protocols/archive/2005/11/10/491563.aspx

3.6.2 Activation du chiffrement SSL dans SafeGuard Enterprise

- Connexion entre le serveur Web et le serveur de base de données

  Le chiffrement SSL peut être configuré en enregistrant le serveur SafeGuard Enterprise à l'aide de l'outil de package de configuration SafeGuard Management Center.

  Pour plus de détails, voir *Enregistrement et configuration du serveur SafeGuard Enterprise* à la page 52.

- Connexion entre le serveur de base de données et SafeGuard Management Center

  Le chiffrement SSL peut être configuré dans l'assistant de configuration de SafeGuard Management Center.

  Pour plus de détails, voir *Configuration de SafeGuard Management Center* à la page 29.

- Connexion entre le serveur SafeGuard Enterprise et l'ordinateur final protégé par SafeGuard Enterprise

  Le chiffrement SSL peut être activé lors de la création du package de configuration pour le client SafeGuard Enterprise à l'aide de l'outil de package de configuration SafeGuard Management Center.

  Pour plus de détails, voir *Création d'un package de configuration de client SafeGuard Enterprise (géré)* à la page 85.

3.7 Étapes d'installation pour SafeGuard Enterprise

Pour installer SafeGuard Enterprise avec la gestion centralisée via SafeGuard Management Center, veuillez procéder comme suit.

	Étape	Description	Package d'installation/ de configuration	Chapitre
1	Mesures préparatoires	Préparations sur le client et le serveur.		*3.1*
2	Configurer l'authentification SQL pour le responsable de la sécurité de SafeGuard Enterprise	Le compte utilisateur est créé sur le serveur Microsoft SQL.		*4.4*
3	Génération de la base de données à l'aide d'un script (facultatif)	Générer les bases de données SafeGuard Enterprise à l'aide d'un script.	Scripts SQL sur le CD du produit dans le répertoire Outils	*4.5.2*
4	Configuration de SafeGuard Management Center	Installer SafeGuard Enterprise Management Center sur le PC de l'administrateur.	SGNManagement Center.msi	*5.2*
5	Configuration de base, générer la base de données à l'aide de l'assistant	Configurer les connexions à la base de données, générer les bases de données SafeGuard Enterprise et le responsable principal de la sécurité.	Assistant de configuration de SafeGuard Management Center	*5.3. 5.4*
6	Configurer le serveur IIS pour SafeGuard Enterprise	Configuration d'IIS avec .NET Framework 3.0 et ASP.NET 2.0		*6.2*
7	Configurer le serveur SafeGuard Enterprise	Installer le serveur SafeGuard Enterprise sur serveur Web IIS.	SGNServer.msi	*6.3*

	Étape	Description	Package d'installation/ de configuration	Chapitre
8	Enregistrer et configurer le serveur SafeGuard Enterprise	Générer le package de configuration du serveur et le déployer sur le serveur Web.	SGNServerConfig.msi Package de configuration du serveur généré dans l'outil de package de configuration SafeGuard Management Center	*6.4*
9	Test de la connexion	Contrôler et établir la connexion entre le serveur, la base de données et SafeGuard Management Center.		*7*
10	Création/Importation d'une structure organisationnelle	Créer une structure ou importer un active directory dans SafeGuard Management Center.		*9*
11	Installer les ordinateurs finaux	Fournir aux ordinateurs finaux la configuration requise pour une installation réussie du logiciel de chiffrement (obligatoire).	SGxClientPreinstall.msi	*10-12*
		Installer le package d'installation du client SafeGuard sur l'ordinateur final. Installer avec ou sans Device Encryption.	SGNClient.msi SGNClient_x64.msi SGNClient_withoutDE.msi SGNClient_withoutDE_x64.msi	*10-12*
		Installer en plus la protection de la configuration (en option).	SGN_CP_Client.msi SGN_CP_Client_x64.msi	*14*

	Étape	Description	Package d'installation/ de configuration	Chapitre
12	Configurer les ordinateurs finaux	Générer le package de configuration pour les ordinateurs finaux gérés ou autonomes et l'installer sur l'ordinateur final.	SGNClientConfig.msi Package de configuration du client généré dans l'outil de package de configuration SafeGuard Management Center	*11.6*

3.8 Étapes d'installation du client SafeGuard Enterprise sur plusieurs systèmes d'exploitation (système d'exécution)

	Étape	Description	Package d'installation/ de configuration	Chapitre
1	Installer le système d'exécution sur l'ordinateur final	Installer le package d'exécution du client SafeGuard sur les volumes d'amorçage secondaires de l'ordinateur final.	SGNClientRuntime.msi SGNClientRuntime_x64.msi	*13*
2	Installer le logiciel de chiffrement SafeGuard sur les ordinateurs finaux	Fournir aux ordinateurs finaux la configuration requise pour une installation réussie du logiciel de chiffrement (obligatoire).	SGxClientPreinstall.msi	*10-12*
		Installer le package d'installation SafeGuard Device Encryption sur le volume d'amorçage primaire de l'ordinateur final.	SGNClient.msi SGNClient_x64.msi	
3	Configurer les ordinateurs finaux	Générer le package de configuration pour les ordinateurs finaux gérés ou autonomes et l'installer sur l'ordinateur final.	SGNClientConfig.msi Package de configuration du client généré dans l'outil de package de configuration SafeGuard Management Center	*11.6*

4 Configuration de la base de données SafeGuard Enterprise

Ce chapitre décrit la configuration d'une base de données SafeGuard Enterprise. Il décrit l'authentification du serveur de base de données nécessaire pour générer une base de données SafeGuard Enterprise. Il propose également des informations sur les droits d'accès SQL requis.

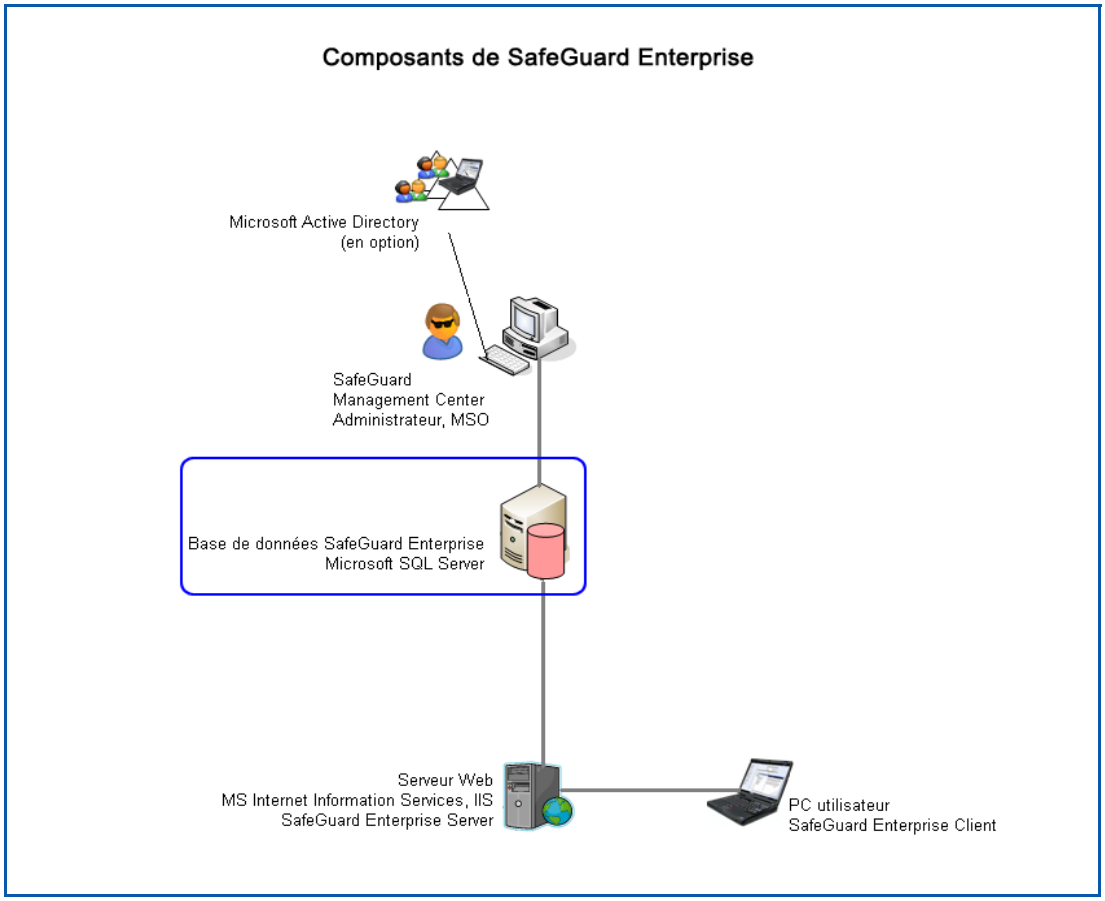
La base de données SafeGuard Enterprise est une base de données SQL basée sur Microsoft SQL Server. Elle contient toutes les données pertinentes, telles que les clés/certificats, les informations sur les utilisateurs et les ordinateurs, les événements et les paramètres de stratégie. Elle peut être générée de deux façons :

- par le principal responsable de la sécurité de SafeGuard Enterprise lors de l'installation de SafeGuard Management Center, à l'aide de l'assistant de configuration de SafeGuard Management ;
- par un administrateur SQL à l'aide d'un script.

Afin d'améliorer les performances, la base de données SafeGuard Enterprise peut être dupliquée sur plusieurs serveurs SQL. Pour configurer la réplication de la base de données, voir *Réplication de la base de données SafeGuard Enterprise* à la page 61.

Plusieurs bases de données SafeGuard Enterprise propres à un locataire peuvent être créées et conservées identiques sur différents locataires, dans le cas par exemple de plusieurs locaux d'entreprise, unités organisationnelles ou domaines. Pour une configuration Multi Tenancy, voir *Configuration de plusieurs bases de données (Multi Tenancy)* à la page 34.

Avant de générer la base de données SafeGuard Enterprise, vous devez configurer un compte utilisateur SQL pour celle-ci.



Avis : nous recommandons d'effectuer une sauvegarde en ligne permanente de la base de données. Sauvegardez régulièrement votre base de données pour protéger les clés, les certificats d'entreprise et les attributions utilisateur-ordinateur. Exemples de cycles de sauvegarde recommandés : après la première importation des données, après des modifications importantes ou à intervalles réguliers, par exemple toutes les semaines ou tous les jours.

4.1 Conditions préalables

Les conditions préalables suivantes doivent être remplies :

- Microsoft SQL Server doit déjà être installé et configuré. Microsoft SQL 2005 Express Edition convient bien aux petites entreprises, car il est exempt de frais de licence.
- Pour des raisons de performances, Microsoft SQL Server et le serveur SafeGuard Enterprise ne doivent pas être installés sur le même ordinateur.
- Les méthodes d'authentification et les droits d'accès pour la base de données doivent être clarifiés.

4.2 Authentification pour la base de données

Pour pouvoir accéder à la base de données SafeGuard Enterprise, le principal responsable de la sécurité de SafeGuard Management Center doit être authentifié. Cette authentification peut être effectuée via :

- l'authentification Windows ;
- l'authentification SQL.

Vous pouvez vous renseigner auprès de votre administrateur SQL pour connaître la méthode d'authentification qui vous est destinée, vous, responsable de la sécurité. Vous avez besoin de cette information avant de générer la base de données et d'installer SafeGuard Management Center.

Utilisez l'authentification SQL pour des ordinateurs ne faisant pas partie d'un domaine, sinon utilisez l'authentification Windows. Ceci nécessite cependant une configuration supplémentaire. Vous trouverez plus d'informations sur l'authentification Windows dans notre base de connaissances (en anglais) :
http://www.sophos.com/support/knowledgebase/article/108339.html.

Si vous utilisez l'authentification SQL, nous conseillons vivement de protéger la connexion de et vers le serveur de base de données avec SSL. Pour plus d'informations, voir *Protection des connexions de transport avec SSL* à la page 11.

4.3 Droits d'accès à la base de données

SafeGuard Enterprise est configuré d'une telle façon que pour utiliser la base de données SQL, vous n'avez besoin que d'un seul compte utilisateur avec des droits d'accès minimaux pour la base de données. Ce compte utilisateur est utilisé par SafeGuard Management Center et délivré uniquement au principal responsable de la sécurité de Management Center. Il garantit la connexion à la base de données SafeGuard Enterprise. Lorsque SafeGuard Enterprise est en cours d'exécution, un seul responsable de la sécurité de SafeGuard Management Center n'a besoin que de l'autorisation en lecture/écriture pour la base de données SafeGuard Management Center.

La base de données SafeGuard Enterprise peut être générée par l'administrateur SQL de l'entreprise ou par le responsable de la sécurité de SafeGuard Management Center. Ce dernier a besoin, pendant un court instant lors de l'installation, de droits d'accès étendus pour la base de données SQL (db_creator) s'il souhaite générer lui-même la base de données SafeGuard Enterprise. Néanmoins, après l'installation, l'administrateur SQL peut révoquer ces droits jusqu'à l'installation ou la mise à jour suivantes.

Si l'extension des autorisations pendant la configuration de SafeGuard Management Center n'est pas souhaitée, l'administrateur SQL peut générer la base de données SafeGuard Enterprise à l'aide d'un script. Les deux scripts contenus sur le CD du produit, CreateDatabase.sql et CreateTables.sql, peuvent être exécutés à cet effet.

Le tableau suivant affiche les autorisations SQL nécessaires pour les différentes versions de Microsoft SQL Server.

Droit d'accès	SQL Server 2005	SQL Server 2005 Express
Génération de la base de données		
Serveur	db_creator	db_creator
Base de données maître	Aucune	Aucune
Base de données SafeGuard Enterprise	db_owner publique (par défaut)	db_owner publique (par défaut)
Utilisation (pas génération) de la base de données		
Serveur	Aucune	Aucune
Base de données maître	Aucune	Aucune
Base de données SafeGuard Enterprise	db_datareader db_datawriter publique (par défaut)	db_datareader db_datawriter publique (par défaut)

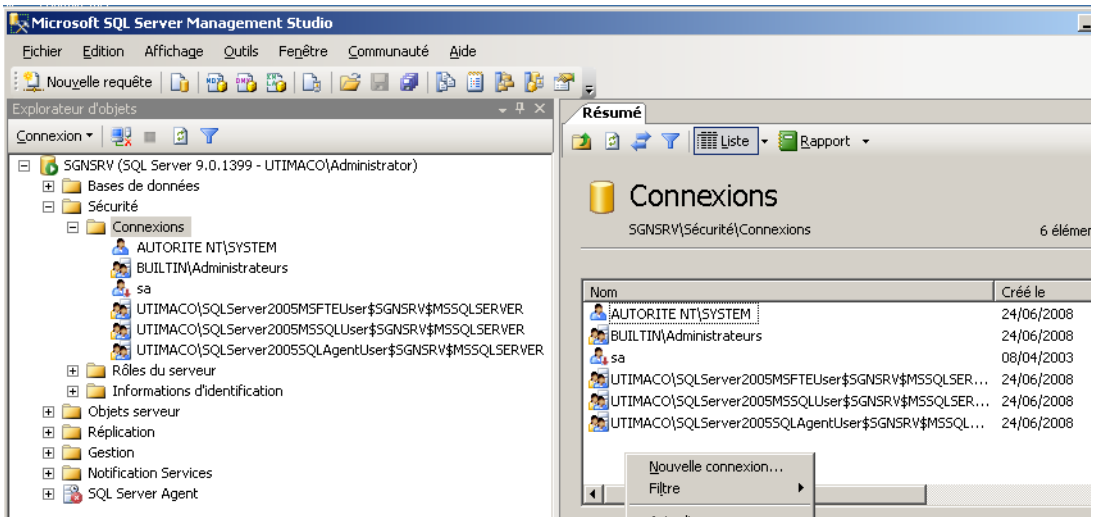
4.4 Configuration d'un compte utilisateur SQL pour SafeGuard Enterprise

Pour générer la base de données SafeGuard Enterprise, un nouvel utilisateur doit être créé dans Microsoft SQL Server pour SafeGuard Enterprise, la méthode d'authentification doit être spécifiée et les droits nécessaires doivent être délivrés.

La description ci-dessous des étapes de configuration est destinée aux administrateurs SQL et concerne Microsoft SQL Server 2005 Express Edition.

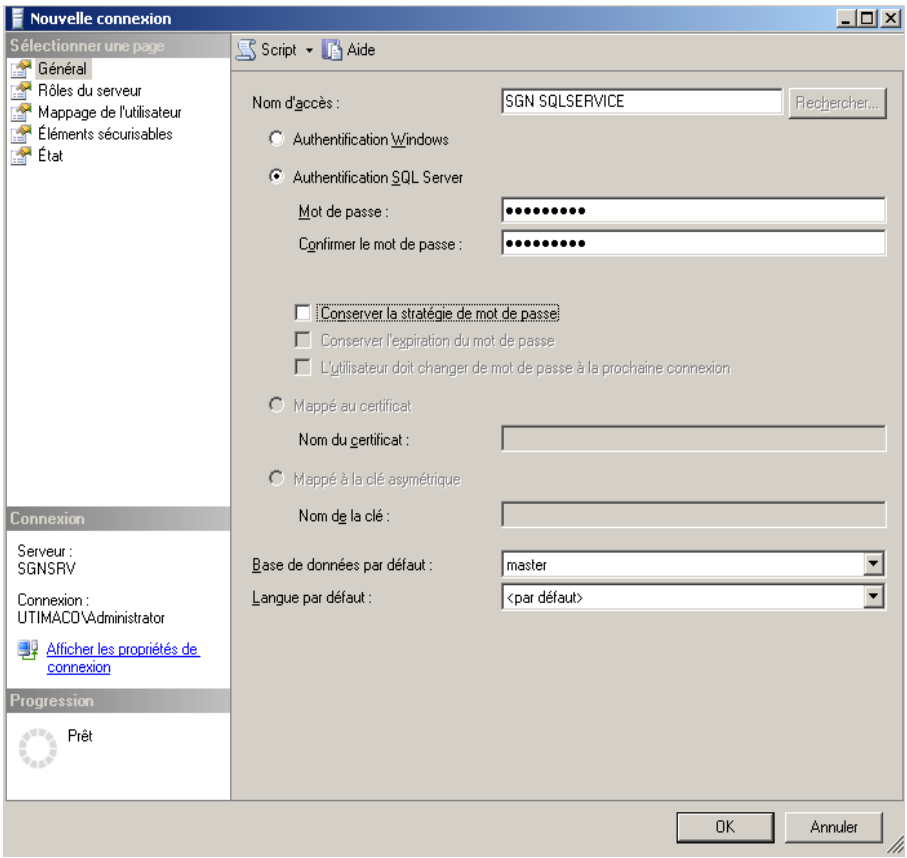
1. Ouvrez le programme SQL Server Management Studio Express. Connectez-vous à SQL Server à l'aide de vos informations d'identification.

2. Dans la fenêtre de navigation de gauche de Microsoft SQL Server Management Studio Express, sélectionnez **Sécurité** > **Connexions**. Dans la fenêtre de droite, cliquez avec le bouton droit sur **Nouvelle connexion**.

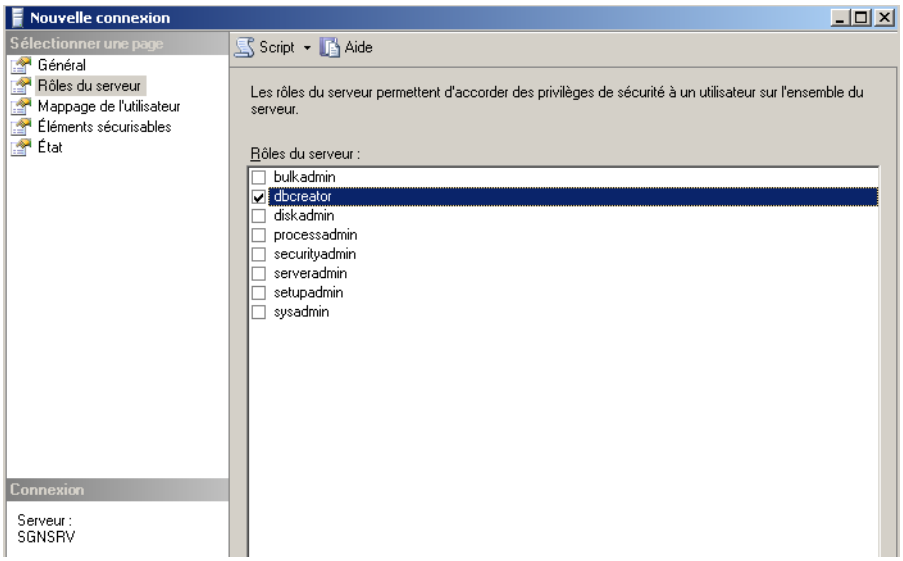


3. Dans **Nouvelle connexion**, sous **Général** :
   - **Nom de connexion** : saisissez le nom du nouvel utilisateur, par exemple SGN SQLSERVICE.
   - Sélectionnez la méthode d'authentification requise (recommandée : authentification SQL) et attribuez un mot de passe.
   - Désactivez **Conserver la stratégie de mot de passe**.
   - **Base de données par défaut** : si aucun script n'a été utilisé pour créer une base de données SafeGuard Enterprise, sélectionnez **maître**.

Plus tard, vous devez informer le responsable de la sécurité de SafeGuard Management Center de la méthode d'authentification et des informations d'identification.



4. À présent, attribuez les droits d'accès/rôles en cliquant à gauche sur **Rôles du serveur** :
   - Pour générer la base de données SafeGuard Enterprise, sélectionnez **dbcreator**. Dès que SafeGuard Enterprise est installé, vous pouvez réinitialiser le rôle de la base de données sur **dbowner**.
   - Si la base de données SafeGuard Enterprise a déjà été créée et sélectionnée en tant que base de données par défaut, sélectionnez **db_datareader**, **db_datawriter** et **publique**.



Le compte utilisateur SQL et les droits d'accès sont maintenant configurés pour le responsable de la sécurité de SafeGuard Enterprise.

4.5 Génération de la base de données SafeGuard Enterprise

Une fois le compte utilisateur SQL configuré, vous devez générer la base de données SafeGuard Enterprise. Pour ce faire, vous pouvez procéder de deux façons.

- via l'assistant de configuration de SafeGuard Management Center

  Cette procédure requiert que SafeGuard Management Center soit déjà installé. Pour cela, voir *Configuration de SafeGuard Management Center* à la page 29.

- via un script SQL disponible sur le CD du produit.

  Cette procédure est généralement préférée si l'extension des autorisations SQL pendant la configuration de SafeGuard Management n'est pas souhaitée.

  La méthode à appliquer dépend de votre environnement. L'administrateur SQL et le responsable de la sécurité SafeGuard Enterprise doivent clarifier ce point.

4.5.1 Génération de la base de données SafeGuard Enterprise via SafeGuard Management Center

Au titre de responsable de la sécurité, vous pouvez facilement générer la base de données SafeGuard Enterprise après l'installation de SafeGuard Management Center. L'assistant de configuration de SafeGuard Management Center vous guide dans la configuration de base qui inclut également la création de la base de données. Pour cela, voir *Configuration de SafeGuard Management Center* à la page 29.

4.5.2 Génération de la base de données SafeGuard Enterprise à l'aide d'un script

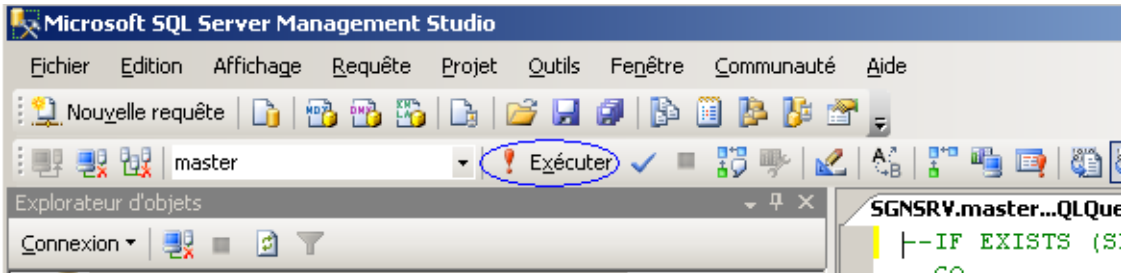
Si l'extension des autorisations SQL pendant la création de la base de données dans Management Center n'est pas souhaitée, vous pouvez également générer la base de données SafeGuard Enterprise à l'aide d'un script. Deux scripts sont fournis à cet effet sur les CD du produit (dossier Outils) :

- CreateDatabase.sql
- CreateTables.sql

La description des étapes ci-dessous est destinée aux administrateurs SQL et concerne Microsoft SQL Server 2005 Express Edition.

1. Ouvrez le script CreateDatabase.sql et vérifiez les deux spécifications de chemins cibles dans **FILENAME**. Elles doivent correspondre aux chemins spécifiés sur le serveur. Corrigez-les si nécessaire.
2. Double-cliquez pour lancer le script CreateDatabase.sql. Microsoft SQL Server Management Studio Express démarre.

3. Connectez-vous à SQL Server à l'aide de vos informations d'identification.
4. Cliquez sur le bouton **Exécuter** pour générer la base de données.



Utilisez maintenant le script CreateTables.sql du CD du produit pour générer les tables.

1. Double-cliquez pour lancer le script CreateTables.sql. Microsoft SQL Server Management Studio Express démarre.
2. Saisissez vos informations d'identification pour SQL Server.
3. Sélectionnez la base de données appropriée que vous avez créée pour SafeGuard Enterprise. Pour ce faire, dans la fenêtre de connexion de SQL Server, cliquez sur **Options** > **Propriétés de connexion**, puis, sous **Connexion à une base de données**, sélectionnez la base de données SafeGuard Enterprise dans laquelle les tables doivent être créées. Cliquez sur **Se connecter**.
4. Cliquez sur le bouton **Exécuter** pour générer les tables.

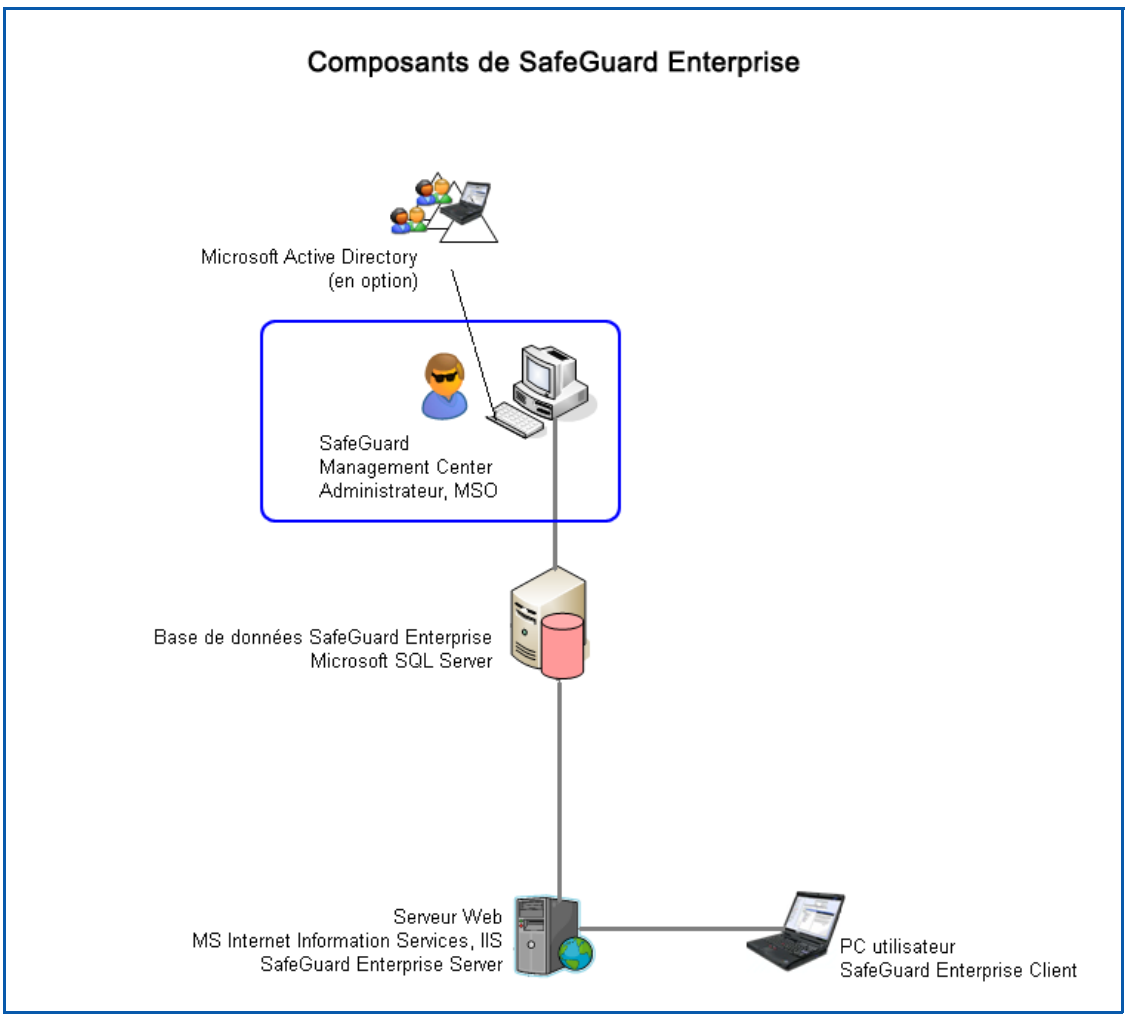
La base de données SafeGuard Enterprise et les tables associées ont été créées.

5 Configuration de SafeGuard Management Center

Ce chapitre décrit l'installation et la configuration de SafeGuard Management Center.

SafeGuard Management Center est l'outil d'administration central de SafeGuard Enterprise. Installez-le sur les PC d'administration que vous souhaitez utiliser pour gérer SafeGuard Enterprise. SafeGuard Enterprise Management Center n'exige pas nécessairement d'être installé sur un seul ordinateur. Il peut être installé sur n'importe quel ordinateur du réseau permettant d'accéder aux bases de données.

SafeGuard Management Center permet de prendre en charge plusieurs bases de données via les configurations de base de données des locataires (**Multi Tenancy**). Vous pouvez configurer et conserver différentes bases de données SafeGuard Enterprise pour différents locataires, dans le cas par exemple de plusieurs locaux d'entreprise, unités organisationnelles ou domaines. Pour faciliter la gestion, les configurations de ces bases de données peuvent également être exportées vers des fichiers et importées à partir de fichiers.



5.1 Conditions préalables

Les conditions préalables suivantes doivent être remplies :

- Vous devez disposer des droits d'administrateur Windows.
- .NET Framework 3.0 Service Pack 1 doit être installé sur le PC d'administration. Vous pouvez le télécharger depuis le site: *http://microsoft.com/downloads*.
- Pour créer une base de données SafeGuard Enterprise pendant la configuration de SafeGuard Management, vous devez disposer des droits d'accès SQL nécessaires (voir *Droits d'accès à la base de données* à la page 19).

5.2 Installation de SafeGuard Management Center

Le package d'installation nécessaire, SGNManagementCenter.msi, se trouve sur le CD du produit.

1. Démarrez SGNManagementCenter.msi à partir du dossier du produit.
2. Cliquez sur **Suivant** dans la fenêtre de bienvenue.
3. Acceptez le contrat de licence.
4. Sélectionnez un chemin d'installation.
5. Sélectionnez le type d'installation :
   - Pour installer SafeGuard Management Center afin de prendre en charge une seule base de données, sélectionnez une installation de type **Classique**.
   - Pour installer SafeGuard Management Center afin de prendre en charge plusieurs bases de données, sélectionnez une installation de type **Personnalisé**. Activez ensuite la fonctionnalité **Multi Tenancy**. Cette fonctionnalité n'est pas installée dans le cas d'une installation de type **Classique**.

     Pour plus d'informations sur la configuration de la fonctionnalité **Multi Tenancy**, voir *Configuration de plusieurs bases de données (Multi Tenancy)* à la page 34.
6. Confirmez la réussite de l'installation.

SafeGuard Management Center est installé. Si nécessaire, redémarrez votre ordinateur.

5.3 Configuration de SafeGuard Management Center

Après l'installation, vous devez configurer SafeGuard Management Center. L'assistant de SafeGuard Management Center propose une assistance conviviale pour la configuration initiale, qui vous aide à spécifier les paramètres de base de Management Center et la connexion à la base de données. Il s'ouvre automatiquement lorsque vous démarrez SafeGuard Management Center pour la première fois après l'installation.

Configurations Multi Tenancy

Vous pouvez configurer différentes bases de données SafeGuard Enterprise et les conserver pour une instance de SafeGuard Management Center. Cela s'avère particulièrement utile pour disposer de configurations de base de données différentes pour différents domaines, unités organisationnelles ou locaux d'entreprise.

Pour faciliter la configuration, des configurations créées précédemment peuvent être importées à partir de fichiers ou de nouvelles configurations de base de données peuvent être exportées, en vue d'une réutilisation ultérieure.

Pour configurer SafeGuard Management pour Multi Tenancy, effectuez d'abord la configuration initiale, puis procédez à la configuration de Multi Tenancy.

Conditions préalables

Vous devez disposer des informations suivantes à portée de main. Si nécessaire, vous pouvez les obtenir auprès de votre administrateur SQL.

- informations d'identification SQL ;
- nom du serveur SQL sur lequel la base de données SafeGuard Enterprise doit s'exécuter ;
- nom de la base de données SafeGuard Enterprise si elle a déjà été créée.

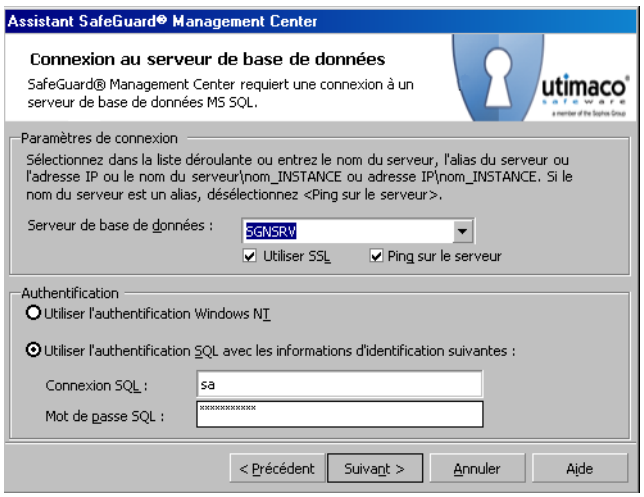
5.4 Réalisation de la configuration initiale

Pour démarrer l'assistant de configuration afin d'effectuer la configuration initiale de SafeGuard Management Center, veuillez procéder comme suit :

Remarque : Vous devez suivre les étapes suivantes pour les configurations Single Tenancy et Multi Tenancy.

1. Démarrez SafeGuard Management Center. L'assistant de configuration de SafeGuard Management Center s'ouvre automatiquement et vous guide dans chacune des étapes à effectuer.

2. Dans **Connexion à la base de données**, configurez la connexion du serveur de base de données :


Assistant SafeGuard® Management Center
Connexion au serveur de base de données
SafeGuard® Management Center requiert une connexion à un serveur de base de données MS SQL.
utimaco
Paramètres de connexion
Sélectionnez dans la liste déroulante ou entrez le nom du serveur, l'alias du serveur ou l'adresse IP ou le nom du serveur\nom_INSTANCE ou adresse IP\nom_INSTANCE. Si le nom du serveur est un alias, désélectionnez <Ping sur le serveur>.
Serveur de base de données :
SGNSRV
Utiliser SSL
Ping sur le serveur
Authentification
Utiliser l'authentification Windows NT
Utiliser l'authentification SQL avec les informations d'identification suivantes :
Connexion SQL :
sa
Mot de passe SQL :
< Précédent
Suivant >
Annuler
Aide

   Dans la liste, sélectionnez le serveur de base de données SQL. La liste de tous les ordinateurs d'un réseau sur lequel Microsoft SQL Server est installé est affichée. Si vous ne pouvez pas sélectionner le serveur, saisissez son nom ou son adresse IP avec le nom de l'instance SQL.

3. Pour que SafeGuard Management Center puisse communiquer avec la base de données, vous devez spécifier une méthode d'authentification pour l'accès à la base de données, soit l'authentification Windows NT, soit l'authentification SQL.

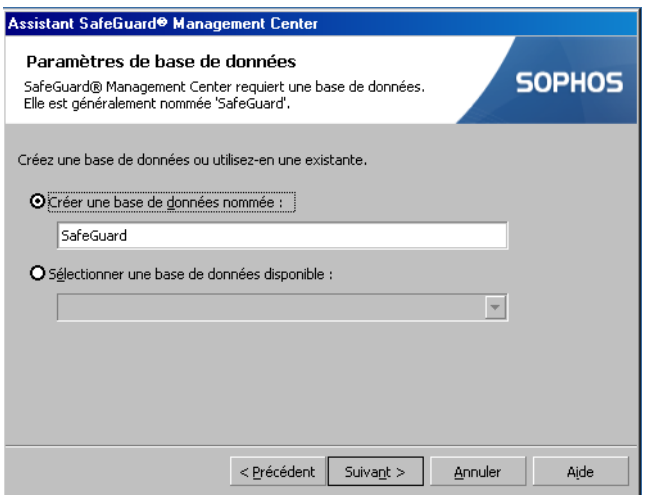
Avis : Utilisez l'authentification SQL pour les ordinateurs ne faisant pas partie d'un domaine, sinon utilisez l'authentification Windows. Toutefois, cela nécessite une configuration supplémentaire.
Si vous utilisez l'authentification SQL, nous vous recommandons vivement de protéger la connexion à la base de données avec SSL afin de chiffrer la transmission des informations d'identification SQL.
Le chiffrement SSL requiert un environnement SSL sur le serveur de base de données SQL que vous avez préalablement configuré ; voir *Protection des connexions de transport avec SSL* à la page 11.

a) Activez **Utiliser l'authentification SQL Server :** saisissez les informations d'identification correspondant au compte utilisateur SQL que votre administrateur SQL a créé. Dans cet exemple, « sa » est utilisé.

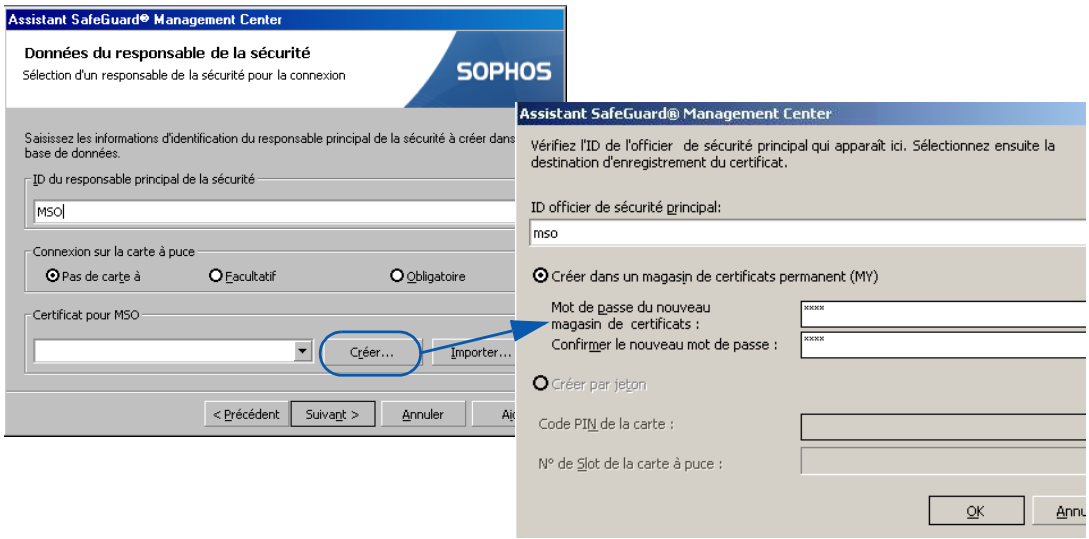
b) Activez **Utiliser SSL** pour protéger la connexion entre SafeGuard Management Center et le serveur de base de données SQL. Si vous avez sélectionné **Authentification SQL Server**, cette option est vivement conseillée pour chiffrer le transport des informations d'identification SQL.

4. Déterminez si une base de données existante ou nouvelle sera utilisée pour stocker les données d'administration.

   - Si aucune base de données n'existe encore, sélectionnez **Créer une base de données nommée**. Saisissez le nom de cette nouvelle base de données, « SafeGuard ». Pour ce faire, vous devez disposer des droits d'accès SQL appropriés (voir *Droits d'accès à la base de données* à la page 19).
   - Si une base de données a déjà été créée ou si vous avez déjà installé Management Center sur un autre PC d'administration, cliquez sur **Sélectionner une base de données disponible**, puis sélectionnez la base de données appropriée dans la liste.


Assistant SafeGuard® Management Center
Paramètres de base de données
SafeGuard® Management Center requiert une base de données.
Elle est généralement nommée 'SafeGuard'.
SOPHOS
Créez une base de données ou utilisez-en une existante.
Créer une base de données nommée :
SafeGuard
Sélectionner une base de données disponible :
< Précédent
Suivant >
Annuler
Aide

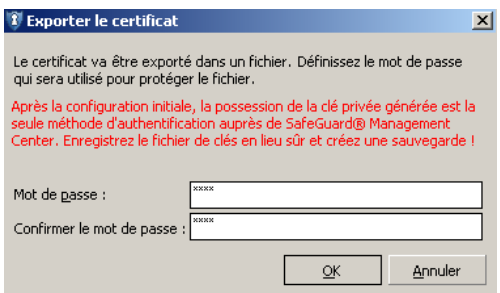
5. Créez un responsable principal de la sécurité (MSO). Saisissez le nom du MSO. Au début, nous recommandons de définir **Connexion sur la carte à puce** sur **Pas de carte à puce**. La connexion avec une clé cryptographique ou une carte à puce nécessite une configuration distincte qui doit être effectuée dans Management Center. Reportez-vous au chapitre relatif aux cartes à puce de l'aide administrateur. Lorsque le nom du MSO a été saisi, cliquez sur **Créer**.


Assistant SafeGuard® Management Center
Données du responsable de la sécurité
Sélection d'un responsable de la sécurité pour la connexion
SOPHOS
Saisissez les informations d'identification du responsable principal de la sécurité à créer dans la base de données.
ID du responsable principal de la sécurité
MSO
Connexion sur la carte à puce
Pas de carte à
Facultatif
Obligatoire
Certificat pour MSO
Créer...
Importer...
< Précédent
Suivant >
Annuler
Assistant SafeGuard® Management Center
Vérifiez l'ID de l'officier de sécurité principal qui apparaît ici. Sélectionnez ensuite la destination d'enregistrement du certificat.
ID officier de sécurité principal:
mso
Créer dans un magasin de certificats permanent (MY)
Mot de passe du nouveau magasin de certificats :
Confirmer le nouveau mot de passe :
Créer par jeton
Code PIN de la carte :
N° de Slot de la carte à puce :
OK

6. Entrez deux fois le mot de passe du certificat et confirmez en cliquant sur **OK**. Le nouveau certificat MSO est enregistré localement sous forme de sauvegarde.

Avis : Notez ce mot de passe. Il s'agit de votre clé privée pour le magasin de certificats de SafeGuard Management. Il vous sera utile par la suite pour vous connecter à Management Center. Il est impossible d'importer un certificat à partir d'une infrastructure de clé publique (PKI) Microsoft.
Un certificat importé doit avoir 1 024 bits au minimum et 4 096 bits au maximum.

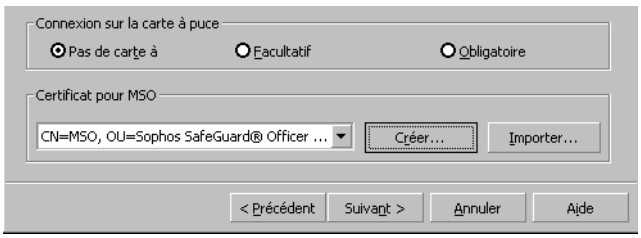
7. Le fichier dans lequel il est stocké (.p12) est sécurisé par un mot de passe. En d'autres termes, cela signifie que le certificat MSO est pourvu d'une protection supplémentaire. Entrez deux fois le mot de passe du fichier .p12 et confirmez en cliquant sur **OK**. Le mot de passe doit être composé de 8 caractères alphanumériques.


Exporter le certificat
Le certificat va être exporté dans un fichier. Définissez le mot de passe qui sera utilisé pour protéger le fichier.
Après la configuration initiale, la possession de la clé privée générée est la seule méthode d'authentification auprès de SafeGuard® Management Center. Enregistrez le fichier de clés en lieu sûr et créez une sauvegarde !
Mot de passe :
Confirmer le mot de passe :
OK
Annuler

8. Entrez un emplacement de stockage pour le certificat.

Avis : Créez une sauvegarde de la clé privée (fichier .p12) pour le MSO, car si la clé est perdue en cas de panne du PC, vous devrez alors réinstaller SafeGuard Enterprise. Ceci est valable pour tous les certificats des responsables de sécurité générés par SafeGuard.

Le certificat MSO a été créé.



9. Cliquez sur **Suivant**.

10. Créez un nouveau certificat d'entreprise. Il sert à différencier les installations SafeGuard Management. Pour des raisons de sécurité, vous devez créer une sauvegarde du certificat de l'entreprise après la configuration initiale sous **Outils** > **Options** > **Certificat** et l'enregistrer en lieu sûr. En association avec le certificat MSO, il permet de restaurer la base de données SafeGuard Enterprise corrompue. Entrez le nom de votre choix.

Assistant SafeGuard® Management Center
Certificat d'entreprise
Créer ou restaurer le certificat global de votre entreprise
SOPHOS
Créer un nouveau certificat d'entre
Saisissez le nom d'entreprise à enregistrer dans le certificat d'entreprise. Il est utilisé pour distinguer visuellement différentes installations.
my_company
Restaurer à l'aide d'un certificat d'entreprise existant
Sujet :
Numéro de série
Date d'expiration
Importer...
< Précédent
Suivant >
Annuler
Aide

11. Cliquez sur **Suivant**, puis sur **Terminer**.

    Un fichier de configuration est alors automatiquement créé.

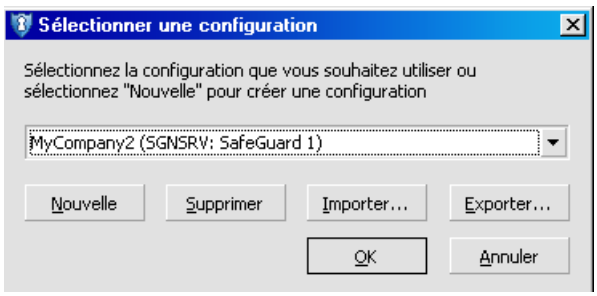
La configuration initiale de SafeGuard Management Center est à présent terminée. SafeGuard Management Center s'ouvre automatiquement.

5.5 Configuration de plusieurs bases de données (Multi Tenancy)

Pour configurer d'autres configurations de base de données afin d'utiliser la fonctionnalité Multi Tenancy, veuillez procéder comme suit.

Condition préalable : La fonctionnalité Multi Tenancy doit avoir été installée via une installation de type Personnalisé. La configuration initiale doit avoir été effectuée (voir *Réalisation de la configuration initiale* à la page 30).

1. Démarrez SafeGuard Management Center.
2. La configuration de base de données existante créée lors de la configuration initiale est affichée. Sélectionnez la tâche à effectuer :



   - Pour créer une autre configuration de base de données SafeGuard Enterprise, cliquez sur **Nouveau**.
   - Pour travailler sur une base de données existante, sélectionnez-la dans la liste déroulante et cliquez sur **OK**.
   - Pour importer une configuration de base de données existante à partir d'un fichier, cliquez sur **Importer...**
   - Pour enregistrer une configuration de base de données dans un fichier, cliquez sur **Exporter...**
3. Effectuez la tâche sélectionnée.

5.5.1 Création de configurations de base de données supplémentaires

Pour créer d'autres configurations de base de données SafeGuard Enterprise à la suite de la configuration initiale, veuillez procéder comme suit :

1. Démarrez SafeGuard Management Center. La boîte de dialogue **Sélectionner une configuration** s'affiche.
2. Cliquez sur **Nouvelle**. L'assistant de configuration de SafeGuard Management Center s'affiche automatiquement.

3. L'assistant vous guide lors des étapes de création d'une nouvelle configuration de base de données ; voir *Réalisation de la configuration initiale* à la page 30. Définissez les paramètres tels que requis. La nouvelle configuration de base de données est générée.
4. Pour vous authentifier dans SafeGuard Management Center, vous êtes invité à sélectionner le nom du responsable de la sécurité de cette configuration et à saisir son mot de passe de magasin de certificats. Confirmez en cliquant sur **OK**.

SafeGuard Management Center est ouvert et relié à la nouvelle configuration de base de données. Au prochain lancement de SafeGuard Management Center, vous pourrez sélectionner la nouvelle base de données dans la liste.

5.5.2 Association à une configuration de base de données existante

Pour travailler sur une configuration de base de données existante, veuillez procéder comme suit :

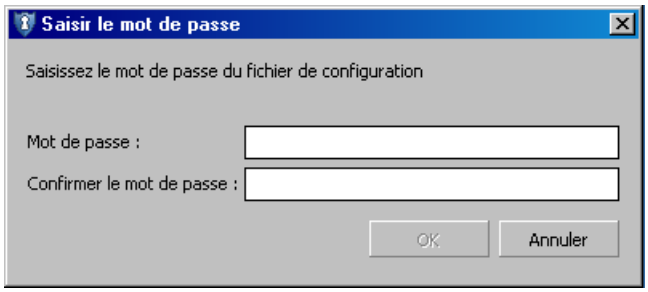
1. Démarrez SafeGuard Management Center. La boîte de dialogue **Sélectionner une configuration** s'affiche.
2. Sélectionnez la configuration de base de données souhaitée dans la liste déroulante et cliquez sur **OK**. La configuration de base de données sélectionnée est reliée à Management Center et activée.
3. Pour vous authentifier dans SafeGuard Management Center, vous êtes invité à sélectionner le nom du responsable de la sécurité de cette configuration et à saisir son mot de passe de magasin de certificats. Confirmez en cliquant sur **OK**.

SafeGuard Management Center est ouvert et relié à la configuration de base de données sélectionnée.

5.5.3 Exportation d'une configuration dans un fichier

Pour enregistrer une configuration de base de données et la réutiliser ultérieurement, vous pouvez l'exporter dans un fichier. Pour cela, veuillez procéder comme suit :

1. Démarrez SafeGuard Management Center. La boîte de dialogue **Sélectionner une configuration** s'affiche.
2. Cliquez sur **Exporter...**
3. Pour protéger le fichier de configuration, vous êtes invité à saisir et confirmer un mot de passe qui chiffrera le fichier de configuration. Cliquez sur **OK**.


Saisir le mot de passe
Saisissez le mot de passe du fichier de configuration
Mot de passe :
Confirmer le mot de passe :
OK
Annuler

4. Spécifiez un nom de fichier et un emplacement de stockage pour le fichier de configuration exportée *.SGNConfig.
5. Si cette configuration existe déjà, vous êtes invité à confirmer le remplacement de la configuration existante.

La configuration de base de données est enregistrée à l'emplacement de stockage spécifié.

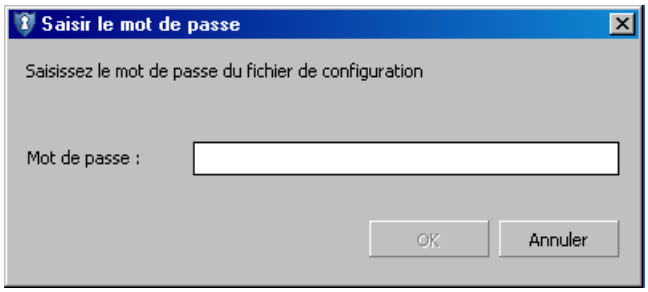
5.5.4 Importation d'une configuration

Pour utiliser ou modifier une configuration de base de données, vous pouvez importer une configuration créée précédemment dans SafeGuard Management Center. Pour ce faire, vous pouvez procéder de deux façons :

- via SafeGuard Management Center (Multi Tenancy) ;
- en double-cliquant sur le fichier de configuration (Single et Multi Tenancy).

5.5.5 Importation d'une configuration via SafeGuard Management Center

1. Démarrez SafeGuard Management Center. La boîte de dialogue **Sélectionner une configuration** s'affiche.
2. Cliquez sur **Importer...**, recherchez le fichier de configuration souhaité, puis cliquez sur **Ouvrir**.
3. Entrez le mot de passe du fichier de configuration défini lors de l'exportation, puis cliquez sur **OK**.



4. La configuration sélectionnée s'affiche. Confirmez pour l'activer en cliquant sur **OK**.
5. Pour vous authentifier dans SafeGuard Management Center, vous êtes invité à sélectionner le nom du responsable de la sécurité de cette configuration et à saisir son mot de passe de magasin de certificats. Confirmez en cliquant sur **OK**. SafeGuard Management Center s'ouvre.

SafeGuard Management Center est ouvert et relié à la configuration de base de données importée.

5.5.6 Importation d'une configuration en double-cliquant sur le fichier de configuration (Single et Multi Tenancy)

Avis : Notez que cette tâche est possible en mode Single Tenancy et Multi Tenancy.

Il est également possible d'exporter une configuration et de la distribuer vers plusieurs responsables de la sécurité. Les responsables de la sécurité double-cliquent alors simplement sur le fichier de configuration pour ouvrir une instance SafeGuard Management Center totalement configurée.

Ceci est avantageux lorsque vous utilisez l'authentification SQL pour la base de données et pour éviter que chaque administrateur connaisse le mot de passe SQL. Vous ne le saisissez ensuite qu'une seule fois, vous créez un fichier de configuration et vous le distribuez vers les ordinateurs des responsables de la sécurité concernés.

Condition préalable : La configuration initiale de SafeGuard Management Center doit avoir été effectuée. Pour plus d'informations, reportez-vous au manuel d'installation de SafeGuard Enterprise.

1. Démarrez SafeGuard Management Center par l'intermédiaire du dossier du produit dans le menu **Démarrer**.
2. Sélectionnez **Options** dans le menu **Outils**, puis cliquez sur l'onglet **Connexion à la base de données**.
3. Saisissez et confirmez les informations d'identification de la connexion au serveur de base de données SQL.
4. Cliquez sur **Exporter la configuration** pour exporter cette configuration vers un fichier.
5. Entrez et confirmez le mot de passe du fichier de configuration.
6. Entrez un nom de fichier et spécifiez un emplacement de stockage.
7. Distribuez ce fichier de configuration vers les ordinateurs des responsables de la sécurité. Fournissez-leur le mot de passe de ce fichier et du magasin de certificats nécessaires pour s'authentifier dans SafeGuard Management Center.
8. Les responsables de la sécurité double-cliquent simplement sur le fichier de configuration.
9. Ils sont invités à saisir le mot de passe du fichier de configuration.
10. Pour s'authentifier à SafeGuard Management Center, ils sont invités à saisir leur mot de passe de magasin de certificats.

SafeGuard Management Center démarre avec la configuration importée et celle-ci devient la nouvelle configuration par défaut.

5.5.7 Basculement rapide entre les configurations de base de données

Pour simplifier la gestion de plusieurs titulaires, SafeGuard Management Center permet de basculer rapidement entre les configurations de base de données.

Pour passer à une autre configuration de base de données :

1. Dans Management Center, sélectionnez **Changer la configuration...** dans le menu **Fichier**.
2. Dans la liste déroulante, sélectionnez la base de données à laquelle vous souhaitez accéder.
3. Cliquez sur **OK**.

Management Center redémarre automatiquement avec la configuration sélectionnée.

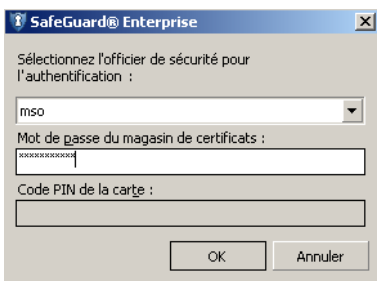
Avis : Notez que cette tâche est également possible en mode Multi Tenancy.

5.6 Connexion à SafeGuard Management Center

La connexion à SafeGuard Management Center dépend du mode d'exécution : Single Tenancy ou Multi Tenancy.

5.6.1 Connexion en mode Single Tenancy

1. Démarrez SafeGuard Management Center via le menu **Démarrer**.
2. Une boîte de dialogue de connexion s'affiche.



3. Connectez-vous en tant que MSO et saisissez le mot de passe du magasin de certificats spécifié durant la configuration initiale. Cliquez sur **OK**.

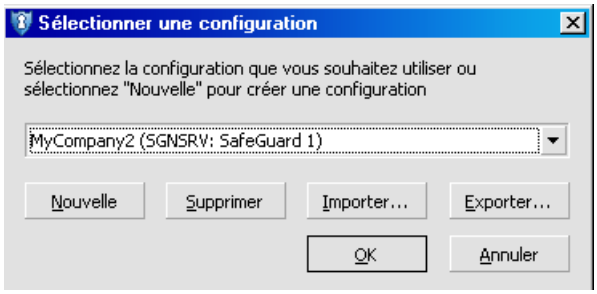
Remarque : Si vous saisissez un mot de passe incorrect, un message d'erreur s'affiche et un délai est imposé avant la tentative de connexion suivante. Le délai est augmenté à chaque échec de tentative de connexion. Les échecs sont consignés.

SafeGuard Management Center est ouvert.

5.6.2 Connexion en mode Multi Tenancy

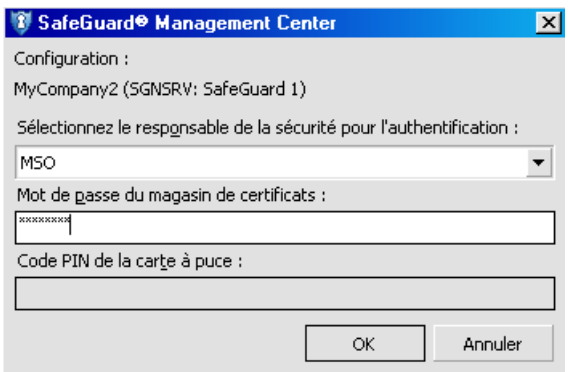
Le processus de connexion à Management Center est plus long lorsque plusieurs bases de données ont été configurées (Multi Tenancy).

1. Démarrez SafeGuard Management Center via le dossier du produit dans le menu **Démarrer**. La boîte de dialogue **Sélectionner une configuration** s'affiche.



2. Sélectionnez la configuration de base de données que vous souhaitez utiliser dans la liste déroulante et cliquez sur **OK**. La configuration de base de données sélectionnée est reliée à Management Center et activée.

3. Pour vous authentifier dans SafeGuard Management Center, vous êtes invité à sélectionner le nom du responsable de la sécurité de cette configuration et à saisir son mot de passe de magasin de certificats. Confirmez en cliquant sur **OK**.



SafeGuard Management Center est ouvert et relié à la configuration de base de données sélectionnée.

Remarque : Si vous saisissez un mot de passe incorrect, un message d'erreur s'affiche et un délai est imposé avant la tentative de connexion suivante. Le délai est augmenté à chaque échec de tentative de connexion. Les échecs sont consignés.

Pour connaître les premières étapes dans SafeGuard Management Center, reportez-vous a l'aide administrateur de SafeGuard Enterprise.

5.7 Installation de SafeGuard Management Center sur d'autres ordinateurs

SafeGuard Enterprise Management Center n'exige pas nécessairement d'être installé sur un seul ordinateur. Il peut être installé sur n'importe quel ordinateur du réseau permettant d'accéder aux bases de données.

SafeGuard Enterprise gère les droits d'accès à Management Center dans son propre répertoire de certificats. Ce répertoire doit contenir tous les certificats de tous les responsables de sécurité autorisés à se connecter à Management Center. La connexion à Management Center ne nécessite ensuite que le mot de passe du magasin de certificats.

Les étapes suivantes correspondent à la configuration d'une seconde installation de Management Center.

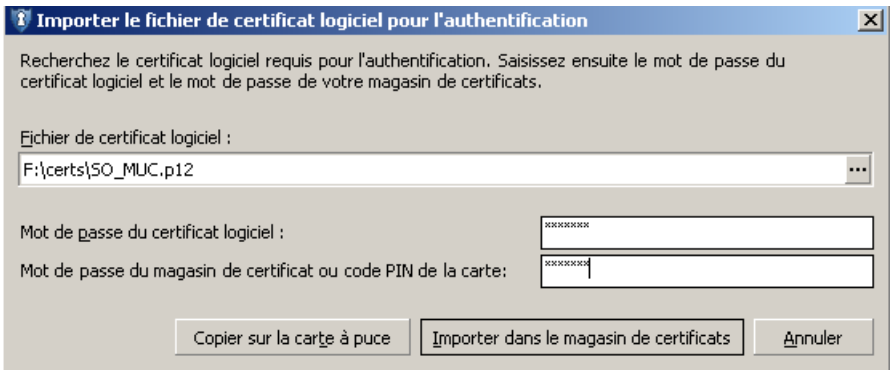
1. Installez SGNManagementCenter.msi sur un autre ordinateur avec les fonctionnalités requises.
2. Ouvrez SafeGuard Management Center. L'assistant de configuration démarre.
3. Sélectionnez la base de données à laquelle cette instance de Management Center doit être connectée.
4. La boîte de dialogue d'**authentification de SafeGuard Management Center** s'affiche. Sélectionnez une personne autorisée dans la liste déroulante. Si le mode Multi Tenancy est activé, la boîte de dialogue Authentification s'affiche pour la configuration à laquelle l'utilisateur est sur le point de se connecter.
5. À présent, saisissez le mot de passe du magasin de certificats.

Avis : Après avoir saisi ce mot de passe, un magasin de certificats est créé pour le compte utilisateur actuel et il est protégé par ce mot de passe. Pour les connexions futures, vous n'avez besoin que de ce mot de passe.

6. Cliquez sur **OK**.

   Un message s'affiche indiquant que le certificat et la clé privée n'ont pas été trouvés ou sont inaccessibles.

7. Pour importer les données, cliquez sur **Oui**.


Importer le fichier de certificat logiciel pour l'authentification
Recherchez le certificat logiciel requis pour l'authentification. Saisissez ensuite le mot de passe du certificat logiciel et le mot de passe de votre magasin de certificats.
Fichier de certificat logiciel :
F:\certs\SO_MUC.p12
Mot de passe du certificat logiciel :
Mot de passe du magasin de certificat ou code PIN de la carte:
Copier sur la carte à puce
Importer dans le magasin de certificats
Annuler

8. Cliquez sur **OK**. Cette opération démarre le processus d'importation.
9. Cliquez sur [**...**] pour sélectionner le fichier de clé.
10. Entrez maintenant le **mot de passe du fichier de clés**.
11. Entrez le mot de passe du magasin de certificats défini précédemment dans **Mot de passe du magasin de certificat ou code PIN de la carte**.
12. Cliquez sur **Importer dans le magasin de certificats**.
    Cliquez sur **Copier sur la carte à puce** pour enregistrer le certificat sur une clé cryptographique.
13. Vous devez saisir le mot de passe une nouvelle fois pour initialiser le magasin de certificats.

Les certificats et les clés privées sont à présent contenus dans le magasin de certificats.

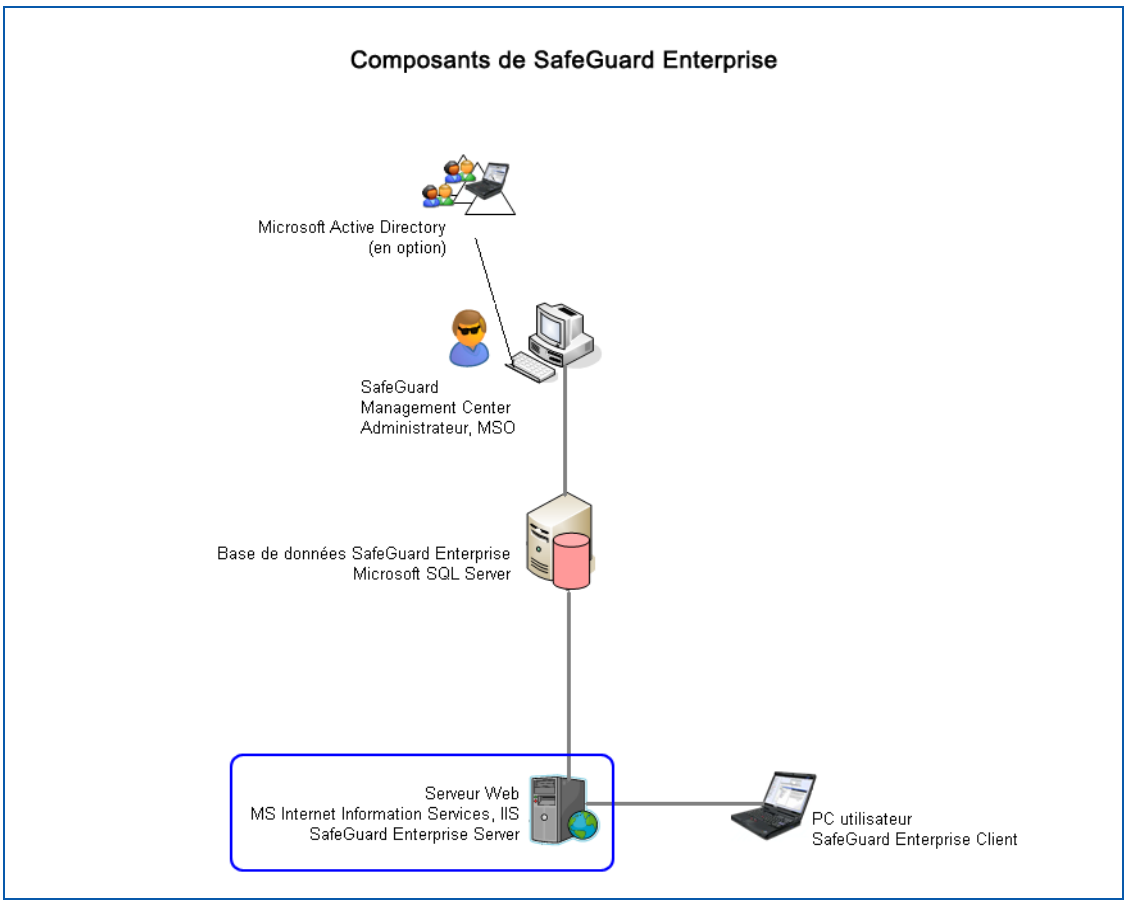
La connexion à SafeGuard Management Center nécessite ensuite le mot de passe du magasin de certificats.

6 Configuration du serveur SafeGuard Enterprise

Le serveur SafeGuard Enterprise sert d'interface avec les clients SafeGuard Enterprise. Comme SafeGuard Management Center, il permet d'accéder à la base de données. Il s'exécute en tant qu'application sur un serveur Web IIS.

Nous recommandons d'utiliser un serveur IIS dédié pour le serveur SafeGuard Enterprise. Les performances s'en trouvent ainsi améliorées. En outre, il garantit l'absence de conflits des autres applications avec SafeGuard Enterprise, par exemple par rapport à la version d'ASP.NET à utiliser.

Ce chapitre décrit l'installation du serveur SafeGuard Enterprise sur un serveur IIS. Pour ce faire, vous devez d'abord configurer Microsoft Internet Information Services (IIS).



6.1 Conditions préalables

Les conditions préalables suivantes doivent être remplies (dans cet ordre) :

- Vous devez disposer des droits d'administrateur Windows.
- Microsoft Internet Information Services (IIS) doit être installé et renforcé.

  IIS est gratuit. Vous trouverez ce programme sur votre CD de Windows ou sur le site Web Microsoft.
- Si vous utilisez le chiffrement de transport SSL entre le serveur SafeGuard Enterprise et le client Enterprise, vous devez configurer IIS au préalable de façon appropriée. Pour cela, voir *Protection des connexions de transport avec SSL* à la page 11 :
  - Un certificat doit être généré et le serveur IIS configuré pour utiliser SSL et sélectionner le certificat.
  - Le nom du serveur spécifié lors de la configuration du serveur SafeGuard Enterprise doit être identique à celui spécifié dans le certificat SSL. Sinon, le client et le serveur ne peuvent pas communiquer. Un certificat distinct est nécessaire pour chaque serveur SafeGuard Enterprise.
  - Si vous utilisez un équilibreur de charge réseau, vérifiez que la plage de ports inclut le port SSL.
- .NET Framework 3.0 Service Pack 1 est installé.

  .NET Framework est gratuit. Vous trouverez ce programme sur votre CD de Windows. Selon la version Windows de votre ordinateur, il a peut-être déjà été installé par défaut.
- ASP.NET 2.0 est activé. L'activation est automatiquement effectuée et correctement définie au moment de l'installation.
- Pour Windows Server 2008, l'option **Scripts et outils de gestion IIS** doit être activée.

6.2 Configuration de Microsoft Internet Information Services (IIS)

Ce chapitre décrit la méthode de préparation du serveur Microsoft Internet Information Services (IIS) à être exécuté avec SafeGuard Enterprise Server.

6.2.1 Renforcement du serveur IIS

Afin d'améliorer la sécurité de l'intranet de votre entreprise, il est recommandé de protéger tous les serveurs IIS et les applications qui y sont exécutées à l'aide des paramètres de sécurité, de manière à ce qu'ils soient « renforcés ».

Ce chapitre décrit la méthode de configuration du serveur IIS de manière à ce qu'il utilise SafeGuard Enterprise Server conformément aux recommandations de sécurisation renforcée de Microsoft. Si d'autres paramètres sont activés et non recommandés par Microsoft ou non conformes aux explications de ce chapitre, les résultats obtenus risquent d'être incorrects.

Remarque : vous trouverez des informations détaillées sur la sécurisation renforcée des serveurs Web dans le Guide de sécurité Microsoft Solutions for Security and Compliance : Guide de sécurité Windows Server 2003, à télécharger gratuitement depuis le site Web de Microsoft.

Les explications de ce chapitre sont basées sur l'exemple de configuration suivant :

- Serveur 1 :

  Microsoft Windows Server 2003 SP1

  Dernière version de SafeGuard Enterprise Server

  Dernière version de SafeGuard Enterprise Management Center

  Microsoft SQL Server 2005 Express

  IIS doté des composants minimaux

- Serveur 2 :

  Microsoft Windows Server 2003 SP2

  Dernière version de SafeGuard Enterprise Server

  Microsoft SQL Server 2005 Express

  IIS doté des composants minimaux

  Seul le Serveur 2 exécute SafeGuard Enterprise Server (serveur IIS). Si le Serveur 2 est en cours d'utilisation, les services activés pour le Serveur 1 seront automatiquement désactivés.

- Client :

  Client SafeGuard Enterprise

  Dernière version de SafeGuard Management Center

Installation des composants IIS requis

Assurez-vous que seuls les composants IIS importants et requis sont installés, car cela réduit les risques d'attaques du serveur IIS. Désactivez tous les paramètres non requis.

L'ensemble de composants minimal que le serveur IIS doit posséder pour être exécuté avec le serveur SafeGuard Enterprise est le suivant :

- Fichiers communs
- Gestionnaire Internet Information Services (IIS)
- Services World Wide Web

Activation des extensions de service Web importantes

Assurez-vous que seules les extensions de service Web importantes sont activées, car cela réduit les risques d'attaques du serveur IIS. Désactivez tous les paramètres non requis.

Les paramètres nécessaires à l'exécution du serveur IIS avec le serveur SafeGuard Enterprise sont les suivants :

- Extension de service Web :
  ASP.NET v.1.1.4322 **Interdite**
  ASP.NET v.2.50727 **Autorisée**

Mise en place du contenu d'un site Web sur un volume de disque dédié

ISS stocke les fichiers du site Web par défaut dans le dossier suivant :
`<systemroot>\inetpub\wwwroot.`
`<systemroot>` correspond au lecteur sur lequel le système d'exploitation Windows Server 2003 est installé.

Déplacez tous les fichiers et dossiers de génération des sites Web et applications sur des volumes de disque dédiés, indépendants du système d'exploitation. Cette opération permet d'éviter les attaques au cours desquelles l'attaquant envoie des requêtes pour un fichier externe à la structure des répertoires d'un serveur IIS.

Dans le cas de l'exemple de configuration, les éléments sont déplacés comme suit :

- Fichiers Web IIS :

  E:\inetpub

- Fichiers Web du serveur SafeGuard Enterprise :

  F:\mycompany.web

Remarque : une fois les fichiers Web déplacés, vous devez mettre à jour en conséquence les informations du chemin d'accès, dans le gestionnaire IIS.

Définition des autorisations NTFS

Les ordinateurs qui exécutent Windows Server 2003 SP1 étudient les autorisations du système de fichiers NTFS pour déterminer les types d'accès attribués à un utilisateur/processus concernant un fichier/dossier. Vous devez attribuer les autorisations NTFS de manière à autoriser ou à interdire l'accès au site Web à des utilisateurs spécifiques du serveur IIS.

Dans le cas de l'exemple de configuration, les autorisations NTFS minimales sont les suivantes :

Utilisateur/Dossier	Autorisations NTFS pour E:\inetpub	Autorisations NTFS pour F:\mycompany.web
Administrateurs	contrôle total	contrôle total
Système	contrôle total	contrôle total
Utilisateurs	exécution	exécution

Vous pouvez définir un autre compte ou groupe pour les utilisateurs, du moment qu'il est présent sur le serveur IIS. Dans ce cas, vous devez mettre à jour en conséquence le compte IUSR_SRVERNAME sur le serveur IIS.

Les autorisations NTFS concernant les types de fichier sont les suivantes :

Type de fichier	Autorisations NTFS recommandées
Fichiers CGI (.exe, .dll, .cmd, .pl)	Administrateurs (contrôle total) Système (contrôle total) Tout le monde/Utilisateur (exécution)
Fichiers de script (.asp)	Administrateurs (contrôle total) Système (contrôle total) Tout le monde/Utilisateur (exécution)
Fichiers d'inclusion (.inc, .shtm, .shtml)	Administrateurs (contrôle total) Système (contrôle total) Tout le monde/Utilisateur (exécution)
Contenu statique (.txt, .gif, .jpg, .htm, .html)	Administrateurs (contrôle total) Système (contrôle total) Tout le monde/Utilisateur (lecture seule)

Désactivation de l'authentification Windows intégrée

Il est recommandé de désactiver l'authentification Windows intégrée dans IIS pour empêcher l'envoi d'informations d'authentification inutiles.

1. Dans le gestionnaire IIS, double-cliquez sur l'ordinateur local, cliquez avec le bouton droit de la souris sur le dossier **Sites Web**, puis cliquez sur **Propriétés**.
2. Cliquez sur l'onglet **Sécurité de répertoire**, puis, dans la section **Authentification et contrôle d'accès**, cliquez sur **Edition**.
3. Dans la section **Accès authentifié**, décochez la case **Authentification intégrée de Windows**.
4. Cliquez deux fois sur **OK**.

Paramètres du pool d'applications DefaultAppPool

- Si le serveur SQL réside sur le même ordinateur que le serveur IIS, définissez le compte utilisateur intégré Service local pour DefaultAppPool. Dans le cas de l'exemple de configuration, il s'agit du Serveur 1.
- Si le serveur SQL réside sur un ordinateur autre que celui du serveur IIS, définissez le compte utilisateur intégré Service réseau pour DefaultAppPool. Dans la configuration fournie à titre d'exemple, il s'agit du Serveur 2. Dans le cas contraire, la synchronisation avec le client échouera.

6.2.2 Nom de déploiement IIS

Lors de l'installation IIS, un utilisateur standard est créé sur le serveur IIS. Il dispose des droits standard. Si le serveur SafeGuard Enterprise est installé sur le serveur IIS, un utilisateur SafeGuard IIS standard est créé. Il dispose des droits IIS standard et du nom de connexion : `IUSR_SafeGuardServerUser`. Cela permet de faciliter l'authentification au niveau du serveur IIS au cas où ce dernier serait renommé après installation, puisque le nom de connexion de l'utilisateur IIS SafeGuard concerné est toujours valide.

6.2.3 Test de l'enregistrement de .NET Framework

Vérifiez si .NET Framework 3.0 avec Service Pack 1 est installé sur le serveur IIS.

1. Pour ce faire, ouvrez le **Panneau de configuration**, puis, en fonction du système d'exploitation, sélectionnez **Ajout/Suppression de programmes** ou **Outils d'administration**. Le programme et la version sont indiqués ici.
2. Si nécessaire, installez la version appropriée du programme.

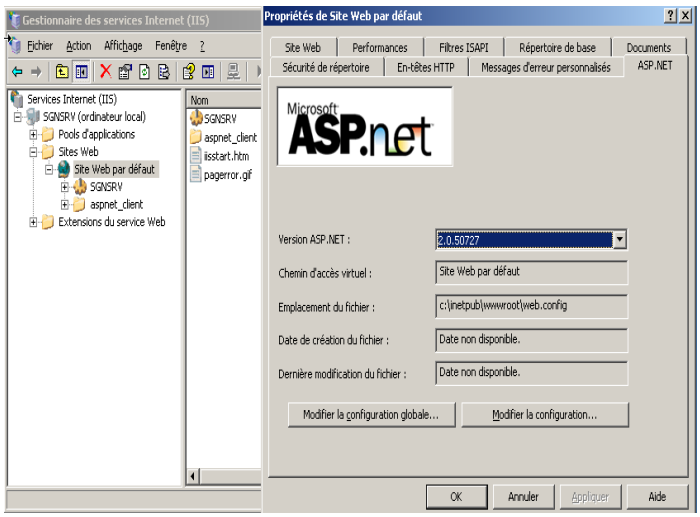
6.2.4 Vérification de l'enregistrement d'ASP.NET

Lors de l'installation du serveur SafeGuard Enterprise, le système vérifie si le service ASP.NET Version 2.0.50727 est défini ou non. S'il n'est pas défini, la version appropriée est automatiquement activée au moment de l'installation.

Vous pouvez vérifier ce réglage manuellement en procédant comme suit :

Remarque : vous trouverez une description détaillée de l'exécution de cette tâche dans notre base de connaissances (en anglais) :
http://www.sophos.com/support/knowledgebase/article/107703.html.

1. Ouvrez le **Gestionnaire des services IIS** sur le serveur IIS.
2. Dans le Gestionnaire des services IIS, cliquez sur **Serveur (ordinateur local) > Sites Web**.
3. Cliquez avec le bouton droit sur **Site Web par défaut > Propriétés > ASP.NET**.
   La version 2.0.50727 doit s'afficher sous **Version ASP.NET**. Sélectionnez cette version si elle est correcte. Si ce n'est pas possible, vous devez réinstaller ASP.Net 2.050727.
4. Pour confirmer, cliquez sur **Appliquer**, puis sur **OK**.



5. Vous pouvez également sélectionner la commande **aspnet_regiis.exe -lv** pour vous assurer de l'installation des services ASP version 2.0.

6.2.5 Configuration IIS 6 supplémentaire lors de l'installation de SafeGuard Enterprise Server sur Windows Server 2003 64 bits

Lorsque vous exécutez IIS version 6 et que vous souhaitez installer SafeGuard Enterprise Server sur Windows Server 2003 64 bits, effectuez les étapes supplémentaires ci-après :

1. Saisissez la commande suivante :

   ```
   cscript %SYSTEMDRIVE%\inetpub\adminscripts\adsutil.vbs SET W3SVC/
   AppPools/Enable32bitAppOnWin64 1
   ```

2. Enregistrez la version ASP.NET requise avec la commande suivante :

   ```
   %SYSTEMROOT%\Microsoft.NET\Framework\v2.0.50727\aspnet_regiis.exe -i
   ```

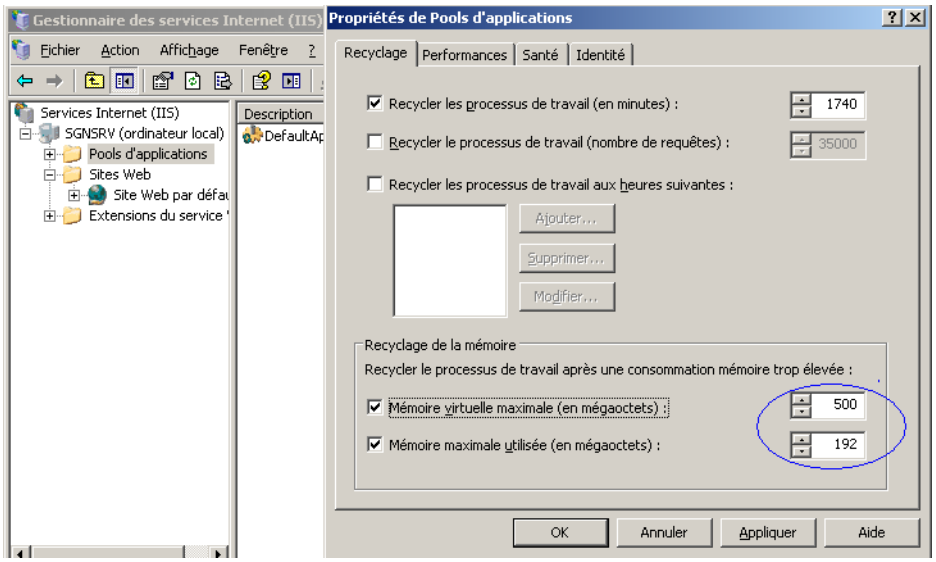
3. Activez la version 32 bits d'ASP.Net 2.0.50727 :

   - Ouvrez le **Gestionnaire des services IIS** sur le serveur IIS.
   - Dans le Gestionnaire des services IIS, cliquez sur **Serveur** (**ordinateur local**) > **Extensions du service Web**.
   - Cliquez avec le bouton droit sur **ASP.NET v2.0.50727** (**32 bits**), sélectionnez **Propriétés** et définissez le statut sur **Autorisé**.
   - Pour confirmer, cliquez sur **Appliquer**, puis sur **OK**.

6.2.6 Activation du recyclage pour le serveur IIS

Nous recommandons de cocher la case « Recycler les processus de travail » pour le serveur IIS :

1. Ouvrez le **Gestionnaire des services IIS**.
2. Dans le Gestionnaire des services IIS, cliquez sur **Serveur** (**ordinateur local**).
3. Cliquez avec le bouton droit sur **Pools d'applications** > **Propriétés**.
4. Sous **Recyclage de la mémoire**, définissez les valeurs suivantes :
   - Mémoire virtuelle maximale = 500 Mo
   - Mémoire maximale utilisée = 192 Mo
5. Pour confirmer, cliquez sur **Appliquer**, puis sur **OK**.



Le serveur IIS est maintenant configuré pour SafeGuard Enterprise.

6.3 Installation du serveur SafeGuard Enterprise

Après avoir configuré IIS, vous pouvez installer le serveur SafeGuard Enterprise sur le serveur IIS. Le package d'installation, SGNServer.msi, se trouve sur le CD du produit.

1. Démarrez `SGNServer.msi` à partir du CD du produit.
2. Cliquez sur **Suivant** dans la fenêtre de bienvenue.
3. Acceptez le contrat de licence.
4. Sélectionnez un chemin d'installation.
5. Confirmez la réussite de l'installation.

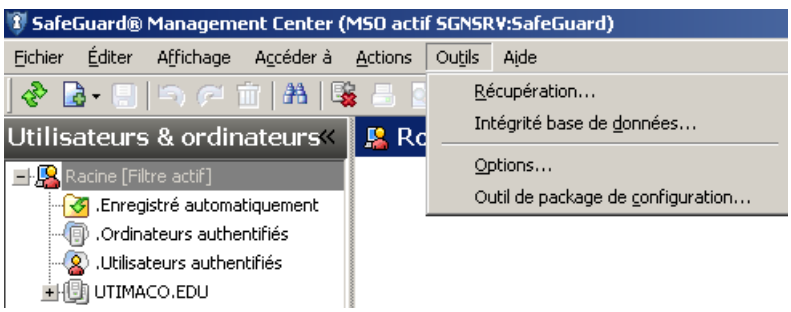
Le serveur SafeGuard Enterprise est installé.

Avis : afin d'améliorer les performances, une fois le serveur SafeGuard Enterprise installé, la concaténation des événements consignés est désactivée par défaut pour la base de données SafeGuard Enterprise.
Toutefois, sans concaténation, aucune protection d'intégrité n'est appliquée aux événements consignés. La concaténation rassemble sous forme de chaînes toutes les entrées du tableau des événements, de manière à ce que la suppression éventuelle d'une entrée soit clairement visible et puisse être contrôlée à l'aide d'une vérification de l'intégrité. Pour utiliser la protection d'intégrité, vous devez donc définir manuellement la concaténation. Pour plus d'informations, reportez-vous au chapitre Rapports de l'aide de l'administrateur de SafeGuard Enterprise.

6.4 Enregistrement et configuration du serveur SafeGuard Enterprise

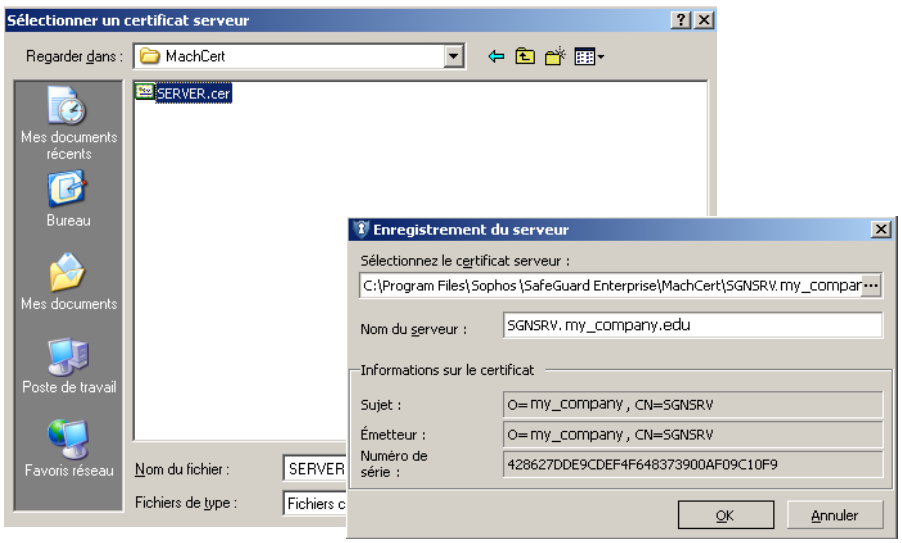
Il est toujours nécessaire d'enregistrer et de configurer le serveur SafeGuard Enterprise. Pour cela, utilisez l'Outil de package de configuration SafeGuard Management Center. Un fichier de configuration doit être créé pour le serveur et déployé sur celui-ci.

1. Démarrez Management Center, puis sélectionnez **Outils** > **Outil du package de configuration**.



2. Sélectionnez **Enregistrer le serveur**, puis l'une des options suivantes :
   - **Faire de cet ordinateur un serveur SGN :** SafeGuard Management Center et le serveur SafeGuard Enterprise sont installés sur le PC sur lequel vous êtes en train de travailler. Cette option n'est pas disponible si la fonctionnalité Multi Tenancy est activée.
   - **Ajouter :** le serveur SafeGuard Enterprise est installé sur un autre PC que SafeGuard Management Center.
   - **Ajouter un rôle serveur :** ajoute si nécessaire des rôles de responsable de sécurité pour le serveur sélectionné.
   - **Supprimer :** le serveur SafeGuard Enterprise est supprimé de la liste.

3. Sélectionnez le certificat machine du serveur, qui est généré lors de l'installation de SafeGuard Enterprise Server. Par défaut, il est situé dans le répertoire **MachCert** du répertoire d'installation de SafeGuard Enterprise Server. Son nom de fichier est `<Nomordinateur>.cer`. Si le serveur SafeGuard Enterprise est installé sur un autre ordinateur que SafeGuard Management Center, ce fichier .cer doit être accessible sous la forme d'une copie ou d'une autorisation réseau.



Avis : ne sélectionnez pas le certificat MSO.

4. Sous **Nom du serveur**, saisissez le nom de domaine entièrement qualifié (FQDN), par exemple, server.mycompany.edu, puis confirmez en cliquant sur **OK**.

Avis : si vous utilisez le chiffrement de transport SSL entre le client et le serveur, le nom du serveur spécifié ici doit être identique à celui spécifié dans le certificat SSL, faute de quoi le client et le serveur ne pourront pas communiquer.

5. Vous avez sélectionné **Faire de cet ordinateur un serveur SGN** :

   a) La configuration du serveur SafeGuard Enterprise démarre automatiquement.

   b) Validez toutes les boîtes de dialogue qui suivent.

L'ordinateur est enregistré comme serveur SafeGuard Enterprise.

6. Le serveur et ses propriétés sont affichés dans l'onglet **Enregistrer le serveur**.

Vous pouvez définir les propriétés suivantes pour le serveur sélectionné :

- **Scripts autorisés :** Activez pour autoriser l'utilisation de l'API de SafeGuard Enterprise Management.
- **Rôles du serveur :** Cliquez pour sélectionner un rôle de responsable de la sécurité. Cliquez sur **Ajouter un rôle serveur...** au bas pour ajouter d'autres rôles de responsable de la sécurité.
- **Connexion à la base de données :** Cliquez sur [...] pour configurer une connexion à une base de données spécifique pour un serveur Web enregistré, notamment les informations d'identification de base de données et le chiffrement de transport SSL entre le serveur Web et le serveur de base de données. La boîte de dialogue **Connexion à la base de données** s'affiche.

Remarque : le chiffrement SSL requiert un environnement SSL et une configuration supplémentaire. Pour cela, voir *Configuration de SSL* à la page 12.

7. Dans **Connexions à la base de données**, configurez la connexion entre la base de données et le serveur :

   a) Sélectionnez le serveur de base de données souhaité et le serveur SafeGuard Enterprise auquel il doit être connecté.

   b) Activez **Utiliser SSL** pour protéger via SSL la connexion entre cette base de données et le serveur sélectionné.

   c) Dans **Authentification**, définissez les informations d'identification de base de données à utiliser pour la base de données sélectionnée :

   - l'authentification Windows ;
   - l'authentification SQL.

Avis : utilisez l'authentification SQL pour les ordinateurs ne faisant pas partie d'un domaine, sinon utilisez l'authentification Windows. Cela nécessite cependant une configuration supplémentaire.
Si vous utilisez l'authentification SQL, nous vous recommandons vivement de sécuriser la connexion à la base de données avec SSL afin de chiffrer la transmission des informations d'identification SQL.

d) Vérifiez la connexion à la base de données. Un nouveau package de configuration serveur peut être créé même si la vérification échoue.

Remarque : vous pouvez modifier à tout moment les propriétés et les paramètres d'un serveur enregistré quel qu'il soit et de sa connexion à la base de données. L'assistant de configuration Management Center ne doit pas être relancé pour mettre à jour la configuration de la base de données. Veillez simplement à créer un nouveau package du serveur ensuite et à le distribuer au serveur concerné. La nouvelle connexion à la base de données peut être utilisée une fois le package du serveur à jour installé sur le serveur.

8. Vous avez sélectionné **Ajouter** :

   a) Ouvrez l'onglet **Créer un package de configuration de serveur**.

   b) Sélectionnez le serveur requis.

   c) Spécifiez le chemin de sortie.

   d) Cliquez sur **Créer un package de configuration**. Un fichier de configuration de serveur (.msi) nommé `<Serveur>.msi` est créé au niveau du chemin de sortie (dans notre exemple, server.mycompany.edu.msi).

Vous avez terminé l'enregistrement et la configuration du serveur SafeGuard Enterprise. Déployez le package de configuration serveur sur le serveur SafeGuard Enterprise.

Avis : si vous souhaitez installer un nouveau package de configuration de serveur, veillez à désinstaller le fichier ServerConfig.msi plus « ancien » avant d'installer un nouveau ServerConfig.msi sur le serveur.

7 Test de la communication

Une fois que le serveur SafeGuard Enterprise, la base de données et SafeGuard Management Center ont été configurés, vous devez exécuter un test de connexion. Ce chapitre décrit les étapes requises.

7.1 Conditions préalables

Définissez ou vérifiez les paramètres suivants avant de tester la connexion :

Ports/connexions

Les PC d'utilisateur doivent créer les connexions suivantes :

Connexion avec	via port
Serveur SafeGuard Enterprise	Port 80/TCP

SafeGuard Management Center doit créer les connexions suivantes :

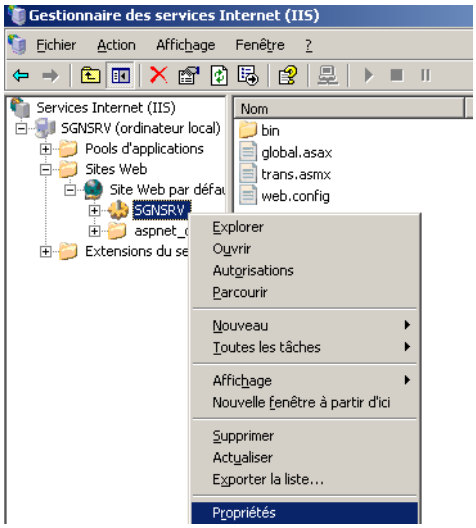
Connexion avec	via port
Base de données SQL	Port 1433/TCP et port 1434/TCP port dynamique pour SQL 2005 (Express)
Active Directory	Port 389/TCP
SLDAP	Port 636 pour l'importation du service Active Directory

Le serveur SafeGuard Enterprise doit créer les connexions suivantes :

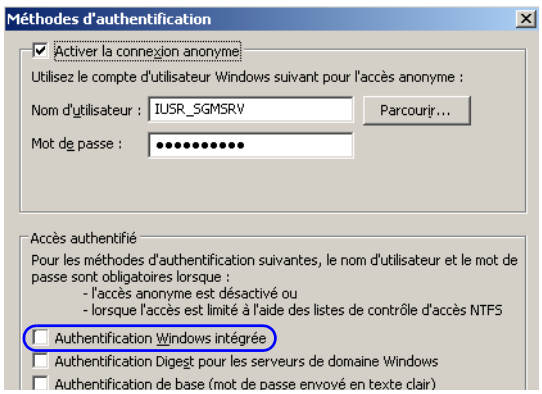
Connexion avec	via port
Base de données SQL	Port 1433/TCP et port 1434/TCP port dynamique pour SQL 2005 (Express)
Active Directory	Port 389/TCP

Méthode d'authentification

1. Sur le serveur SafeGuard Enterprise, ouvrez le **Gestionnaire des services IIS**.
2. Dans l'arborescence, sélectionnez **Internet Information Services** > « **Nomduserveur** » > **Sites Web** > **Site Web par défaut** > **SGNSRV**.
3. Cliquez avec le bouton droit sur **SGNSRV**, puis sélectionnez **Propriétés**.



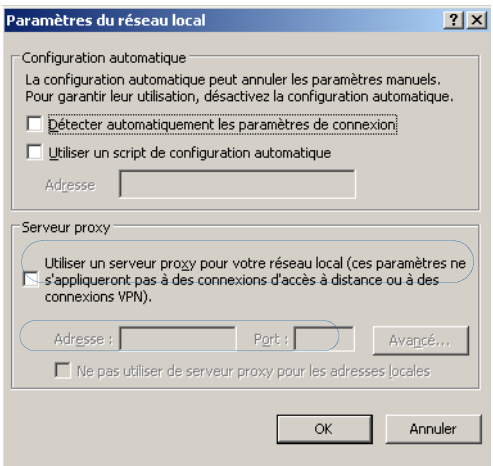
4. Sélectionnez l'onglet **Sécurité de répertoire**.
5. Dans la zone **Authentification et contrôle d'accès**, cliquez sur **Modifier**.
   Sélectionnez **Activer la connexion anonyme** et désélectionnez **Authentification Windows intégrée**.


Méthodes d'authentification
Activer la connexion anonyme
Utilisez le compte d'utilisateur Windows suivant pour l'accès anonyme :
Nom d'utilisateur :
IUSR_SGMSRV
Parcourir...
Mot de passe :
Accès authentifié
Pour les méthodes d'authentification suivantes, le nom d'utilisateur et le mot de passe sont obligatoires lorsque :
- l'accès anonyme est désactivé ou
- lorsque l'accès est limité à l'aide des listes de contrôle d'accès NTFS
Authentification Windows intégrée
Authentification Digest pour les serveurs de domaine Windows
Authentification de base (mot de passe envoyé en texte clair)

Paramètres du serveur proxy pour le serveur Web et le PC d'utilisateur

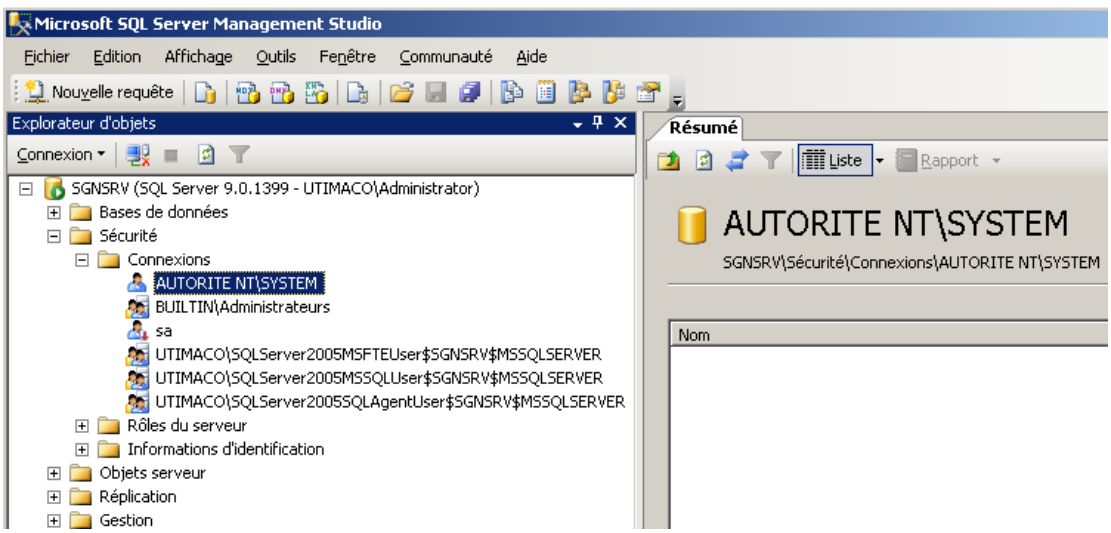
Les paramètres du serveur proxy doivent être définis comme suit :

1. Dans Internet Explorer, sélectionnez **Outils** > **Options Internet** > **Connexions** > **Paramètres réseau.**
2. Désactivez **Utiliser un serveur proxy pour votre réseau local.**
3. Si un serveur proxy est nécessaire, activez **Ne pas utiliser de serveur proxy pour les adresses locales.**


Paramètres du réseau local
Configuration automatique
La configuration automatique peut annuler les paramètres manuels. Pour garantir leur utilisation, désactivez la configuration automatique.
Détecter automatiquement les paramètres de connexion
Utiliser un script de configuration automatique
Adresse
Serveur proxy
Utiliser un serveur proxy pour votre réseau local (ces paramètres ne s'appliqueront pas à des connexions d'accès à distance ou à des connexions VPN).
Adresse :
Port :
Avancé...
Ne pas utiliser de serveur proxy pour les adresses locales
OK
Annuler

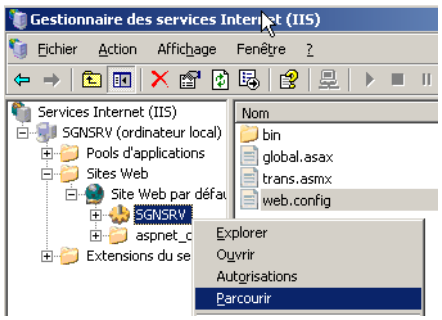
Paramètres de Microsoft SQL Server 2005

Si vous utilisez Microsoft SQL Server 2005, vous devez ajouter les utilisateurs suivants dans Microsoft SQL Server Management Studio (rôle « sysadmin ») :



7.2 Réalisation du test de connexion

1. Sur le serveur SafeGuard Enterprise, ouvrez le **Gestionnaire des services IIS**.
2. Dans le Gestionnaire des services IIS, cliquez sur **Serveur (ordinateur local) > Sites Web > Site Web par défaut**.
3. Cliquez avec le bouton droit sur le serveur souhaité, puis cliquez sur **Parcourir**.

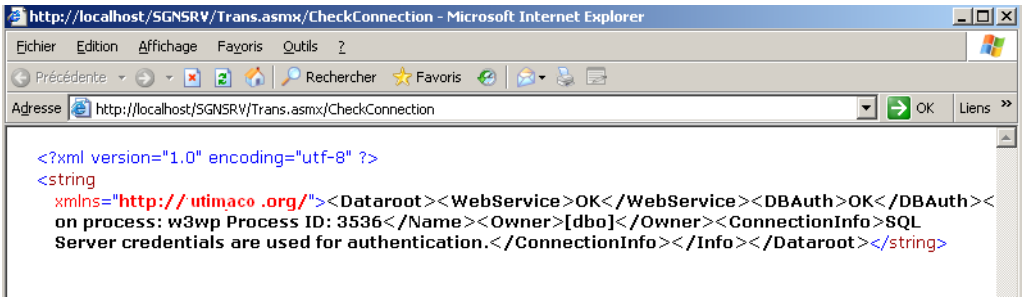


4. Cliquez sur le lien **Vérifier la connexion**.

5. Testez la connexion en cliquant sur **Appeler**.

Le résultat suivant indique que le test de connexion est satisfaisant :

- `WebServices ok`
- `DBAuth ok`



8 Réplication de la base de données SafeGuard Enterprise

Afin d'améliorer les performances, la base de données SafeGuard Enterprise peut être dupliquée sur plusieurs serveurs SQL.

Ce chapitre décrit la méthode de configuration de la réplication pour la base de données SafeGuard Enterprise dans un environnement distribué. Nous considérons que vous avez déjà une certaine expérience concernant l'utilisation du mécanisme de réplication dans Microsoft SQL Server.

Remarque : l'administration doit avoir lieu uniquement sur la base de données principale, et non sur les bases de données dupliquées.

8.1 Réplication de fusion

La réplication de fusion correspond au processus de distribution des données d'un éditeur vers des abonnés. Il permet à l'éditeur et aux abonnés d'effectuer des mises à jour de manière indépendante, puis de les fusionner d'un site à l'autre.

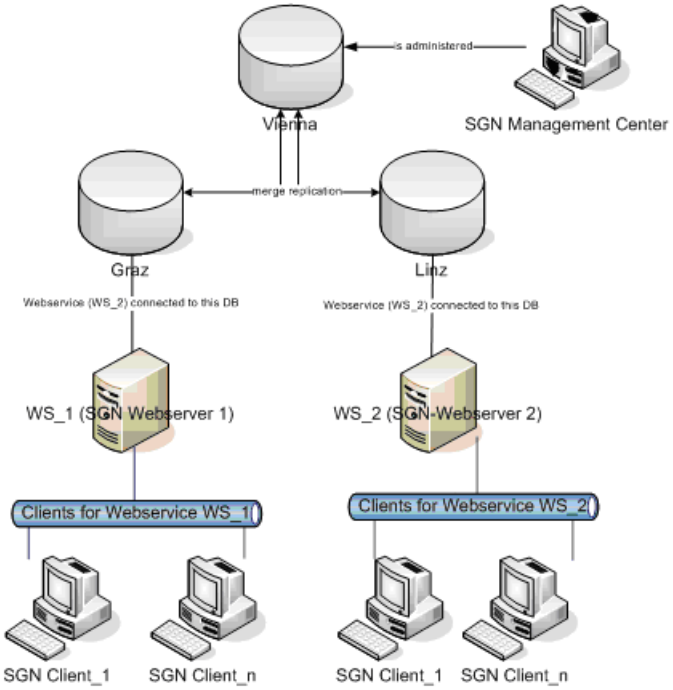
La réplication de fusion permet à plusieurs sites de travailler de façon autonome, puis de fusionner les mises à jour de manière à obtenir un résultat unique et homogène. La capture instantanée initiale est appliquée aux abonnés, puis Microsoft SQL Server effectue un suivi des modifications sur les données publiées par l'éditeur et par les abonnés. Les données sont synchronisées continuellement entre les serveurs, à intervalles réguliers ou sur demande. Puisque les mises à jour sont effectuées sur plusieurs serveurs, les mêmes données peuvent avoir été mises à jour par l'éditeur ou par plusieurs abonnés. Des conflits peuvent donc apparaître lors de la fusion.

La réplication de fusion comprend des choix par défaut et personnalisés de résolution des conflits, que vous pouvez modifier au moment de la configuration d'une publication de fusion. Lorsqu'un conflit survient, un programme de résolution est appelé par l'agent de fusion. Il détermine les données à accepter et à propager vers les autres sites.

8.2 Configuration de la réplication des bases de données

La configuration d'une réplication d'une base de données SafeGuard Enterprise est expliquée à l'aide d'un exemple basé sur Microsoft SQL Server 2005.

Dans l'exemple, SafeGuard Enterprise est administré de manière exclusive depuis la base de données à **Vienne**. Toutes les modifications sont transmises de SafeGuard Management Center aux bases de données **Graz** et **Linz** par réplication dans Microsoft SQL Server 2005. Les modifications signalées par les ordinateurs client via les serveurs Web sont également transmises à Microsoft SQL Server 2005 par réplication.



8.2.1 Génération de la base de données principale

Commencez par configurer la base de données SafeGuard Enterprise principale. Dans notre exemple, il s'agit de la base de données **Vienne**.

La procédure de génération de la base de données principale est la même que pour une installation de SafeGuard Enterprise sans réplication.

Vous pouvez procéder de deux façons :

- via l'assistant de configuration de SafeGuard Management Center

  Cette procédure requiert que SafeGuard Management Center soit déjà installé ; voir *Installation de SafeGuard Management Center* à la page 28.

- via un script SQL disponible sur le CD du produit.

  Cette procédure est généralement préférée si l'extension des autorisations SQL lors de la configuration de SafeGuard Management n'est pas souhaitée (voir *Configuration de la base de données SafeGuard Enterprise* à la page 17).

8.2.2 Génération des bases de données dupliquées Graz et Linz

Une fois la base de données principale configurée, vous pouvez générer les bases de données dupliquées. Dans notre exemple, il s'agit des bases de données Graz et Linz.

Remarque : les tables de données et les tableaux EVENT se trouvent dans des bases de données distinctes. Par défaut, les entrées d'événement ne sont pas concaténées, de manière à ce que la base de données des événements puisse être dupliquée sur plusieurs serveurs SQL afin d'améliorer les performances. Si les tableaux EVENT sont concaténés, des problèmes peuvent survenir lors de la réplication si les données sont enregistrées.

Pour générer les bases de données dupliquées, veuillez procéder comme suit :

1. Lorsque vous utilisez des bases de données distribuées, vous devez d'abord créer une publication de la base de données principale à partir de la console de gestion du serveur SQL.
2. Sélectionnez les tables, les vues et les procédures stockées à synchroniser dans cette publication.
3. Créez les bases de données dupliquées en générant un abonnement pour Graz et un autre pour Linz. Les nouvelles bases de données Graz et Linz apparaissent ensuite également dans l'assistant de configurations des abonnements SQL.
4. Fermez l'assistant de configuration SQL. Le moniteur de réplication indique si la réplication s'exécute correctement ou non.
5. Assurez-vous de saisir le nom de base de données approprié dans la première ligne du script SQL. Par exemple, utilisez `Graz` ou `Linz`.
6. Réalisez à nouveau les captures instantanées à l'aide de l'agent de capture instantanée.

Les bases de données dupliquées Graz et Linz ont été créées. Passez à l'installation du serveur SafeGuard Enterprise.

8.3 Installation et configuration du serveur SafeGuard Enterprise

Pour installer le serveur SafeGuard Enterprise sur les serveurs Web, veuillez procéder comme suit. Pour plus d'informations sur l'installation, voir *Configuration du serveur SafeGuard Enterprise* à la page 43.

1. Installez le serveur SafeGuard Enterprise sur le serveur WS_1.
2. Installez le serveur SafeGuard Enterprise sur le serveur WS_2.
3. Enregistrez les serveurs dans SafeGuard Management Center à l'aide de l'option **Outils** > **Outil de package de configuration** > **Enregistrer le serveur** > **Ajouter**.
4. Vous êtes invité à ajouter les certificats de serveur ws_1.cer et ws_2.cer. Vous les trouverez dans le dossier suivant : `\Program Files\Sophos\SafeGuard Enterprise\MachCert\`. Ces certificats sont nécessaires à la création des packages de configuration du serveur et du client appropriés.

Les serveurs SafeGuard Enterprise sont installés et enregistrés. Vous devez désormais créer les packages de configuration du serveur et du client pour chacun d'entre eux.

8.3.1 Génération des packages de configuration de la base de données Graz

Créez le package de configuration du serveur et du client pour la base de données **Graz**. Démarrez SafeGuard Management Center et veuillez procéder comme suit :

1. Connectez SafeGuard Management Center à la base de données Graz. Dans **Outils** > **Options**, sélectionnez **Connexion à la base de données**, puis `WS_1` comme **Serveur de base de données** et `Graz` comme **Base de données**.
2. Dans **Outils** > **Outil de package de configuration** > **Créer un package de configuration de serveur**, créez le package de configuration du serveur.
3. Dans **Outils** > **Outil de package de configuration** > **Créer un package de configuration** (**géré**), créez le package de configuration pour l'ordinateur final protégé par SafeGuard Enterprise. Assurez-vous de sélectionner le serveur auquel les clients Graz sont connectés. Dans notre exemple, il s'agit de WS_1.

8.3.2 Génération des packages de configuration de la base de données Linz

Pour créer le package de configuration du serveur et du client pour la base de données **Linz**, démarrez SafeGuard Management Center et veuillez procéder comme suit :

1. Connectez SafeGuard Management Center à la base de données Linz. Dans **Outils** > **Options**, sélectionnez **Connexion à la base de données**, puis `WS_2` comme **Serveur de base de données** et `Linz` comme **Base de données**.
2. Dans **Outils** > **Outil de package de configuration** > **Créer un package de configuration de serveur**, créez le package de configuration du serveur.
3. Dans **Outils** > **Outil de package de configuration** > **Créer un package de configuration** (**géré**), créez le package de configuration pour les ordinateurs finaux protégés par SafeGuard Enterprise. Assurez-vous de sélectionner le serveur auquel les clients Linz sont connectés. Dans notre exemple, il s'agit de WS_2.
4. Une fois que vous avez créé les packages de configuration du serveur et du client, reconnectez SafeGuard Management Center à la base de données **Vienne**.

8.3.3 Installation des packages de configuration du serveur

Pour installer les packages de configuration de serveur sur les serveurs Web, veuillez procéder comme suit :

1. Installez le package de configuration du serveur (ws_1.msi) sur le service Web WS_1, destiné à communiquer avec la base de données Graz.
2. Installez le package de configuration du serveur (ws_2.msi) sur le service Web WS_2, destiné à communiquer avec la base de données Linz.

Si les communications entre le serveur SafeGuard Enterprise et ces bases de données fonctionnent correctement, vous pouvez installer les clients SafeGuard Enterprise.

8.4 Installation et configuration du logiciel client SafeGuard Enterprise

L'installation des clients SafeGuard Enterprise se déroule de la même façon que pour SafeGuard Enterprise sans réplication. Pour plus d'informations, voir *Installation centralisée des ordinateurs finaux* à la page 80 ou voir *Configuration locale des ordinateurs finaux* à la page 97.

Pour obtenir la configuration appropriée, veillez à installer le package de configuration du client approprié une fois que vous avez installé chacun des clients SafeGuard Enterprise. Dans le cas de notre exemple, veuillez procéder comme suit :

1. Installez le package de configuration du client Graz sur les clients à connecter au serveur Graz WS_1.

2. Installez le package de configuration du client Linz sur les clients à connecter au serveur Linz WS_2.

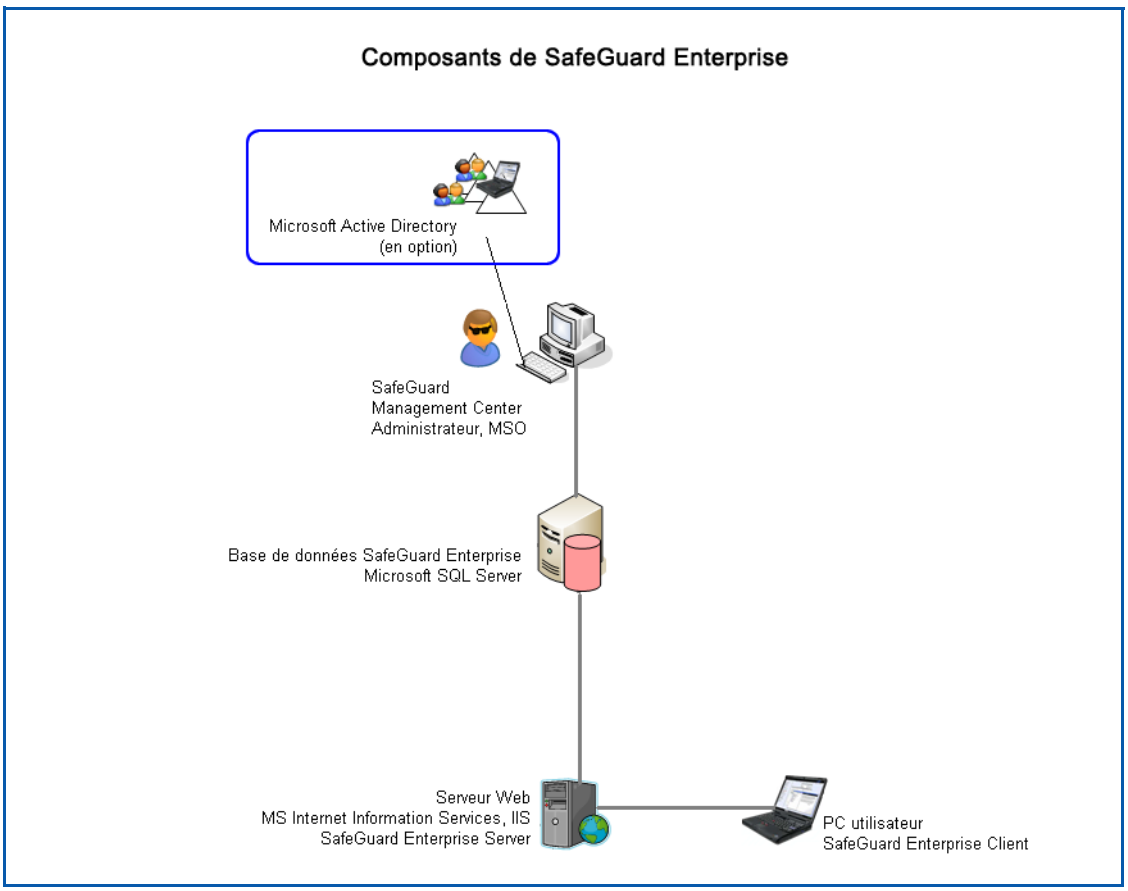
Pour plus d'informations sur la mise à jour des bases de données SafeGuard Enterprise dupliquées, voir *Mise à jour des bases de données dupliquées SafeGuard Enterprise* à la page 112.

9 Configuration d'une structure organisationnelle

Deux méthodes vous permettent de mapper votre organisation dans SafeGuard Enterprise :

- création manuelle de la structure de l'entreprise ;
- importation d'un service d'annuaire, par exemple Active Directory.

Vous pouvez utiliser l'une de ces deux méthodes ou combiner les deux. Par exemple, vous pouvez importer un service Active Directory (AD) partiellement ou intégralement, et créer manuellement d'autres unités organisationnelles. Dans ce cas, les unités organisationnelles créées manuellement ne sont pas mappées dans le service AD.
Pour mapper dans le service AD les unités organisationnelles créées dans SafeGuard Enterprise, ajoutez-les à ce service.



9.1 Création manuelle d'une structure organisationnelle

Si vous ne souhaitez pas importer votre structure organisationnelle à partir d'un service Active Directory ou si aucun service d'annuaire n'est disponible, vous pouvez implémenter manuellement la structure organisationnelle en créant des domaines/groupes de travail auxquels l'utilisateur/ordinateur peut se connecter.

Pour créer un domaine, veuillez procéder comme suit :

Pour l'afficher, ouvrez SafeGuard Management Center, puis cliquez sur **Utilisateurs & ordinateurs**.

1. Sélectionnez **Racine** [**Filtre actif**] dans la fenêtre de navigation de gauche.
2. Dans le menu contextuel, sélectionnez **Nouveau** > **Créer un domaine** (**enregistrement auto**).
3. Saisissez les informations suivantes concernant le contrôleur de domaine dans **Informations communes**. La saisie des trois noms doit être correcte sinon le domaine ne sera pas synchronisé :
   a) **Nom complet** : par exemple *nom ordinateur.domaine.com* ou l'adresse IP du contrôleur de domaine.
   b) **Nom distinctif** : nom DNS, par exemple : `DC=nomordinateur3,DC=domaine,DC=pays`
   c) Description du domaine (facultatif)
   d) **Netbios du domaine :** nom du contrôleur de domaine
   e) Le type d'objet est affiché sous **État de la connexion**, dans ce cas `Domaine`.
   f) Pour empêcher l'héritage de stratégie, vous pouvez activer **Bloquer l'héritage de stratégie**.
4. Confirmez les détails en cliquant sur **OK**.

Pour créer un groupe de travail, veuillez procéder comme suit :

Pour l'afficher, ouvrez SafeGuard Management Center, puis cliquez sur **Utilisateurs & ordinateurs**.

1. Sélectionnez **Racine** [**Filtre actif**] dans la fenêtre de navigation de gauche.
2. Dans le menu contextuel, sélectionnez **Nouveau** > **Créer un groupe de travail** (**enregistrement auto**).
3. Saisissez les informations suivantes dans le champ **Informations communes** :
   a) **Nom complet :** nom du groupe de travail
   b) Description du groupe de travail (facultatif)

c) Le type d'objet est affiché sous **État de connexion**, dans ce cas `Groupe de travail`.

d) Pour empêcher l'héritage de stratégie, vous pouvez activer **Bloquer l'héritage de stratégie**.

4. Confirmez les détails en cliquant sur **OK**.

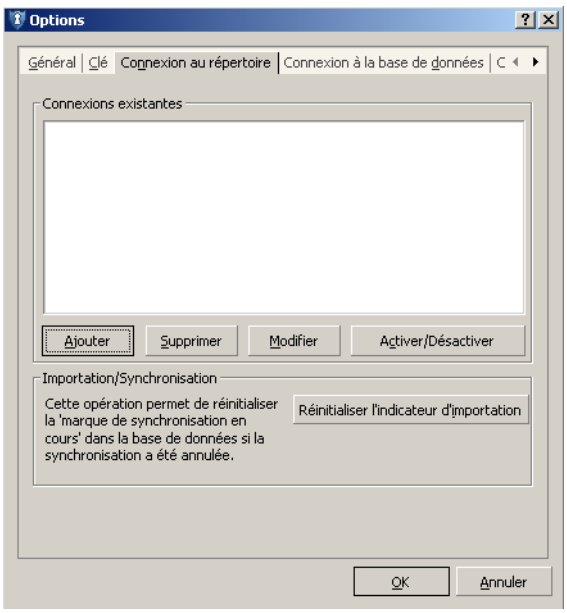
Le nouveau domaine/groupe de travail est à présent créé. Les utilisateurs/ordinateurs de ce domaine sont automatiquement affectés à ce domaine/groupe de travail lorsqu'ils se connectent. Poursuivez de la même façon jusqu'à ce que votre structure organisationnelle soit créée.

9.2 Importation d'une structure organisationnelle

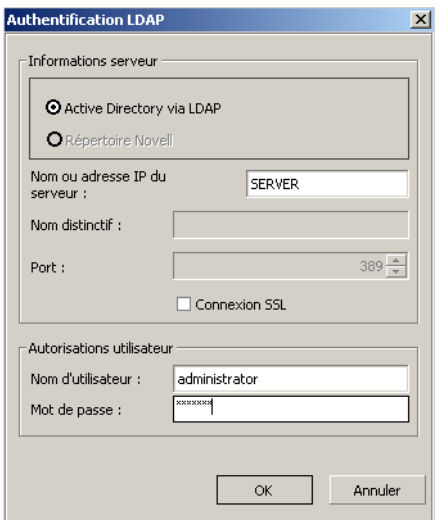
Vous avez la possibilité d'importer une structure organisationnelle existante dans la base de données SafeGuard Enterprise, par exemple via Active Directory.

1. Démarrez SafeGuard Management Center.

2. Sélectionnez **Outils** > **Options** > **Connexion au répertoire** et cliquez sur **Ajouter**.



a) **Authentification LDAP** apparaît.



b) Dans le champ **Nom ou adresse IP du serveur**, saisissez le nom NetBIOS du contrôleur de domaine ou son adresse IP.

c) Dans le champ **Nom d'utilisateur et mot de passe**, saisissez vos informations d'identification Windows.

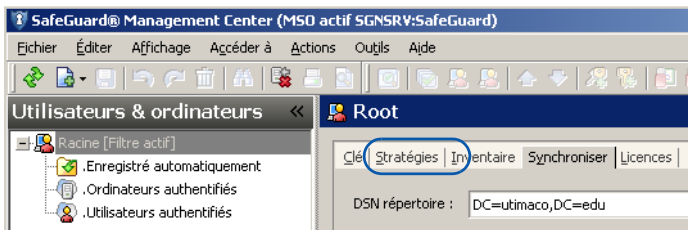
Remarque : Ordinateur unique Windows : Un répertoire doit être approuvé sur le PC pour activer une connexion via LDAP.
Lors de la synchronisation d'utilisateurs avec leur appartenance à un groupe, l'appartenance à un « groupe principal » n'est pas synchronisée, car elle n'est pas visible pour le groupe.

3. Confirmez en cliquant sur **OK**.

4. Cliquez sur **Utilisateurs & ordinateurs**.

5. Dans la fenêtre de navigation de gauche, cliquez sur le répertoire racine **Racine** [**Filtre actif**].

6. Sélectionnez **Synchroniser**.



7. Sélectionnez le répertoire requis dans la liste **DSN**. Cliquez sur l'icône de la loupe, dans l'angle supérieur droit. Une représentation graphique de la structure Active Directory des unités organisationnelles de votre entreprise s'affiche.

8. Il n'est pas nécessaire d'importer l'ensemble du contenu d'Active Directory. Sélectionnez les unités organisationnelles qui doivent être synchronisées.

9. Cliquez sur **Synchroniser**.

10. Confirmez la synchronisation en cliquant sur **OK**.

La synchronisation de SafeGuard Management Center et d'Active Directory est terminée. Les objets importés sont affichés dans la zone **Utilisateurs & ordinateurs**. Vous pouvez afficher un protocole de synchronisation dans la barre d'état à gauche. Vous pouvez copier ce protocole dans le Presse-papiers en cliquant dessus, puis le coller dans un e-mail ou un fichier, au cas où vous souhaiteriez informer vos utilisateurs des résultats de la synchronisation.

10 Configurations de SafeGuard pour les ordinateurs finaux

Vous pouvez configurer les ordinateurs finaux comme suit :

- **En tant que clients SafeGuard Enterprise (gérés)** à l'aide de la gestion centralisée basée sur serveur via SafeGuard Management Center.

  Il existe une connexion au serveur SafeGuard Enterprise pour les clients SafeGuard Enterprise (gérés). Ils reçoivent leurs stratégies via le serveur SafeGuard Enterprise. La connexion peut être désactivée provisoirement, par exemple lors d'un déplacement professionnel, mais même dans ce cas l'ordinateur final est défini comme géré.

- **En tant que clients Sophos SafeGuard (autonomes)** à l'aide de la gestion locale via SafeGuard Management Center.

  Aucune connexion n'est jamais établie avec le serveur SafeGuard Enterprise pour les clients Sophos SafeGuard (autonomes). Ils reçoivent donc leurs stratégies dans des packages de configuration via des mécanismes tiers.

Avis : recherchez la présence éventuelle, sur votre réseau et vos ordinateurs, de packages de configuration obsolètes ou non utilisés et, pour des raisons de sécurité, pensez à les supprimer.

10.1 Restrictions

AHCI

Si Intel AHCI (Advanced Host Controller Interface) est utilisé sur l'ordinateur, le disque dur d'amorçage doit être installé dans le slot 0 ou le slot 1. Vous pouvez insérer jusqu'à 32 disques durs. SafeGuard Enterprise ne fonctionne que sur les deux premiers numéros de slot.

Disques dynamiques et GPT

Les disques dynamiques et GPT (GUID Partition Table) ne sont pas pris en charge. Dans ces cas-là, l'installation est interrompue. Si de tels disques sont trouvés sur l'ordinateur ultérieurement, ils ne sont pas pris en charge.

Disques durs SCSI

Le client SafeGuard Enterprise Device Encryption ne prend pas en charge les systèmes équipés de disques durs reliés par un bus SCSI.

Restrictions pour le chiffrement initial des clients SafeGuard Enterprise (gérés)

La configuration initiale des clients SafeGuard Enterprise (gérés) peut impliquer la création de stratégies de chiffrement pouvant être distribuées aux clients SafeGuard Enterprise sous forme de packages de configuration.

Toutefois, lorsque le client SafeGuard Enterprise ne se connecte pas à un serveur SafeGuard Enterprise juste après l'installation du package de configuration et qu'il est temporairement hors ligne, seules les stratégies de chiffrement présentant les paramètres spécifiques suivants sont immédiatement activées sur le client Enterprise :

- Protection des périphériques basés sur le volume avec la clé machine définie comme clé de chiffrement

Pour que toutes les autres stratégies impliquant le chiffrement à l'aide de clés définies par l'utilisateur soient activées sur le client Enterprise, les packages de configuration correspondants doivent également être réaffectés à l'unité organisationnelle du client Enterprise. Les clés définies par l'utilisateur sont créées uniquement lorsque la connexion entre le client Enterprise et le serveur SafeGuard Enterprise est rétablie.

Cela est dû au fait que la clé machine définie est directement créée sur le client SafeGuard Enterprise lors du premier redémarrage après installation, alors que les clés définies par l'utilisateur ne peuvent être créées sur le client SafeGuard Enterprise qu'une fois que ce dernier a été enregistré sur le serveur SafeGuard Enterprise.

Restrictions pour les clients Sophos SafeGuard (autonomes)

- Les modules suivants ne sont pas pris en charge pour les clients Sophos SafeGuard (autonomes) :
  - Prise en charge de SafeGuard Enterprise BitLocker
  - Configuration Protection

Restrictions pour la prise en charge de BitLocker

- Le package d'installation suivant n'est pas disponible pour les clients SafeGuard Enterprise (gérés) prenant en charge BitLocker :
  - SGNClient_withoutDE.msi/SGNClient_withoutDE_x64.msi

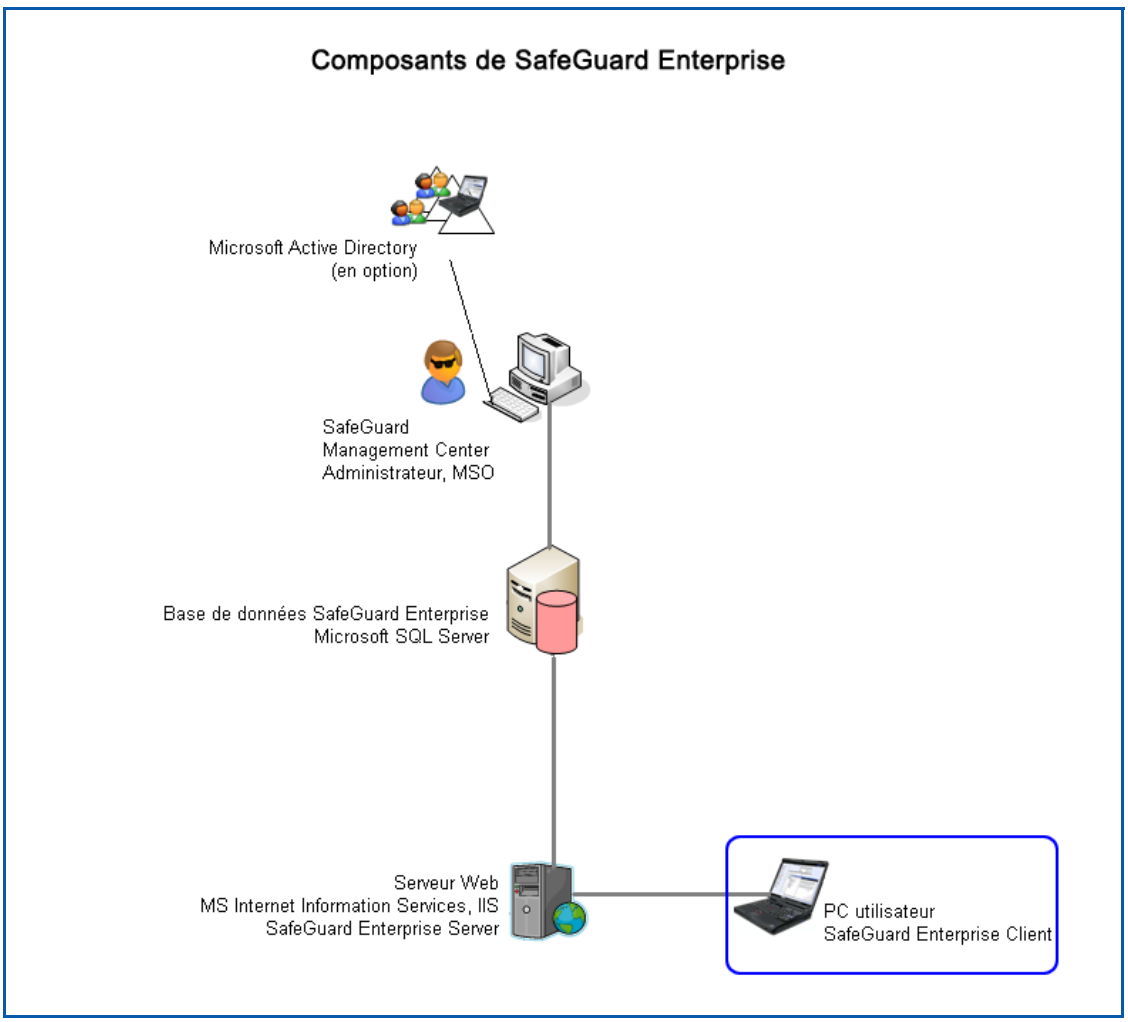
Avis : vous pouvez utiliser le chiffrement basé sur volume de SafeGuard Enterprise ou de BitLocker sur Windows Vista/Windows 7, mais vous ne pouvez pas utiliser simultanément ces deux méthodes. Pour changer de type de chiffrement, vous devez d'abord déchiffrer toutes les partitions, désinstaller le package d'installation du client SafeGuard Enterprise, puis le réinstaller avec les fonctions que vous souhaitez utiliser.

10.2 Clients SafeGuard Enterprise (gérés)

Les clients SafeGuard Enterprise (gérés) sont gérés de manière centralisée dans SafeGuard Management Center.

Il existe une connexion au serveur SafeGuard Enterprise pour les clients SafeGuard Enterprise. La connexion peut être désactivée provisoirement, par exemple lors d'un déplacement professionnel, mais même dans ce cas, l'ordinateur final est toujours défini comme client SafeGuard Enterprise géré.

Le package de configuration requis est créé dans SafeGuard Management Center.



10.2.1 Packages d'installation pour les clients SafeGuard Enterprise (gérés)

Avis : Si vous utilisez le système d'exploitation Windows 7 64 bits ou Windows Vista 64 bits sur les ordinateurs finaux (<nom packaget>_x64.msi), vous pourrez installer la variante 64 bits des packages « client » .msi. Le package 64 bits de SafeGuard Configuration Protection est disponible pour Windows 7 64 bits.

Le tableau suivant répertorie les packages d'installation disponibles pour le client Enterprise et indique comment créer le package de configuration :

Package	Description
SGxClientPreinstall.msi	Doit être installé sur les ordinateurs finaux avant le logiciel de chiffrement (obligatoire). Fournit aux ordinateurs finaux la configuration requise pour une installation réussie du logiciel de chiffrement.
SGNClient.msi **SGNClient_x64.msi**	Destiné aux clients SafeGuard Enterprise et aux clients Enterprise prenant en charge BitLocker. **SafeGuard Enterprise Device Encryption** Chiffrement basé sur volume avec authentification au démarrage **SafeGuard Data Exchange** Facilité d'échange de données avec des supports amovibles sur toutes les plates-formes sans rechiffrement Chiffrement basé sur fichier
SGNClient_withoutDE.msi **SGNClient_withoutDE_x64.msi**	Ce package n'est pas disponible pour les clients SafeGuard Enterprise prenant en charge BitLocker. **SafeGuard Data Exchange** Échange facilité des données avec des supports amovibles sur toutes les plates-formes sans rechiffrement Chiffrement basé sur fichier sans authentification au démarrage
SGN_CP_Client.msi **SGN_CP_Client_x64.msi** (disponible pour Windows 7 64 bits)	Destiné aux clients SafeGuard Enterprise et aux clients Enterprise prenant en charge BitLocker. **Configuration Protection** Protection des ports et gestion des périphériques Le package 64 bits de SafeGuard Configuration Protection est disponible pour Windows 7 64 bits.

Package	Description
SGNClientRuntime.msi **SGNClientRuntime_x64.msi**	Client d'exécution qui permet l'initialisation à partir d'un volume d'amorçage secondaire lorsque plusieurs systèmes d'exploitation sont installés et qui accède à ces volumes lorsqu'ils sont chiffrés par une installation de SafeGuard Enterprise sur le volume primaire. Disponible pour les clients SafeGuard Enterprise et les clients SafeGuard autonomes.
Package de configuration du client Enterprise	Créé dans l'outil du package de configuration de SafeGuard Management Center.

10.3 Clients Sophos SafeGuard (autonomes)

Les clients Sophos SafeGuard (autonomes) ne sont à aucun moment connectés au serveur SafeGuard Enterprise et ne sont pas non plus connectés à la gestion centralisée de SafeGuard Enterprise ; ils fonctionnent donc en mode autonome.

La différence majeure avec un client SafeGuard Enterprise (géré) est qu'un client Sophos SafeGuard (autonome) reçoit les stratégies SafeGuard Enterprise uniquement via un package de configuration. Il ne reçoit jamais de stratégies via une connexion établie avec le serveur SafeGuard Enterprise.

Les clients Sophos SafeGuard (autonomes) sont gérés localement. Les groupes de stratégies et les packages de configuration sont créés dans SafeGuard Management Center. Les packages de configuration sont ensuite distribués par les mécanismes de distribution de logiciels de la société ou installés manuellement sur les ordinateurs finaux.

10.3.1 Restrictions

Les modules suivants ne sont pas pris en charge sur les clients Sophos SafeGuard (autonomes) :

- **Configuration Protection**
- **Prise en charge de BitLocker**

10.3.2 Packages d'installation disponibles pour les clients Sophos SafeGuard (autonomes)

Avis : Pour les packages d'installation client, une variante 64 bits est disponible pour les systèmes d'exploitation Windows 7 64 bits et Windows Vista 64 bits (<nom package>_x64.msi). Si vous utilisez le système d'exploitation Windows 7 64 bits ou Windows Vista 64 bits sur les ordinateurs finaux, vous pourrez installer la variante 64 bits des packages « client » .msi.

Le tableau suivant répertorie les packages d'installation Client disponibles pour ce scénario en mode autonome et indique comment créer le package de configuration :

Package	Description
SGxClientPreinstall.msi	Doit être installé sur les ordinateurs finaux avant le logiciel de chiffrement (obligatoire). Fournit aux ordinateurs finaux la configuration requise pour une installation réussie du logiciel de chiffrement.
SGNClient.msi **SGNClient_x64.msi**	**SafeGuard Enterprise Device Encryption** Chiffrement basé sur volume avec authentification au démarrage **SafeGuard Data Exchange** Facilité d'échange de données avec des supports amovibles sur toutes les plates-formes sans rechiffrement Chiffrement basé sur fichier
SGNClient_withoutDE.msi **SGNClient_withoutDE_x64.msi**	**SafeGuard Data Exchange** Facilité d'échange de données avec des supports amovibles sur toutes les plates-formes sans rechiffrement Chiffrement basé sur fichier sans authentification au démarrage
SGNClientRuntime.msi **SGNClientRuntime_x64.msi**	Client d'exécution qui permet l'initialisation à partir d'un volume d'amorçage secondaire lorsque plusieurs systèmes d'exploitation sont installés et qui accède à ces volumes lorsqu'ils sont chiffrés par une installation de SafeGuard Enterprise sur le volume primaire. Disponible pour les clients SafeGuard Enterprise (gérés) et les clients Sophos SafeGuard (autonomes).
Package de configuration du client autonome	Créé dans l'outil du package de configuration de SafeGuard Management Center.

11 Installation centralisée des ordinateurs finaux

Ce chapitre décrit l'installation centralisée des ordinateurs finaux pour plusieurs ordinateurs.

L'installation et la configuration sont décrites pour les clients SafeGuard Enterprise (gérés) ainsi que pour les clients Sophos SafeGuard (autonomes).

Les tâches requises pour l'installation des ordinateurs d'utilisateur avec Windows BitLocker sont également décrites.

Les responsables de la sécurité SafeGuard Enterprise peuvent exécuter l'installation et la configuration initiale des ordinateurs finaux dans le cadre de la distribution centralisée des logiciels. Cela garantit l'installation standardisée sur plusieurs ordinateurs finaux.

Avis : dans le cadre de la distribution centralisée des logiciels, les packages d'installation et de configuration doivent uniquement être attribués à un ordinateur et non à un utilisateur.

Le comportement des ordinateurs finaux lors de la première connexion après l'installation de SafeGuard Enterprise est décrit dans l'aide de l'utilisateur de SafeGuard Enterprise.

11.1 Conditions préalables générales

Les conditions préalables suivantes doivent être remplies :

- Vous devez disposer des droits d'administrateur Windows.
- Un compte utilisateur doit être configuré et actif sur les ordinateurs finaux.
- La sauvegarde complète des données doit être exécutée sur les ordinateurs finaux.
- Cette condition préalable s'applique uniquement aux clients SafeGuard Enterprise :

  Vérifiez s'il existe une connexion avec le serveur SafeGuard Enterprise. Sur les ordinateurs finaux, sélectionnez cette adresse Web dans Internet Explorer :

  http://<AdresseIPServeur>/sgnsrv

  Si la page Trans affiche **Vérifier la connexion**, la connexion avec le serveur SafeGuard Enterprise est établie.

11.2 Conditions préalables pour BitLocker

Si vous souhaitez utiliser SafeGuard Enterprise pour gérer les ordinateurs finaux BitLocker, vous devez exécuter les tâches de préparation suivantes sur les ordinateurs finaux :

- Windows 7/ Windows Vista Enterprise ou Ultimate doit être installé sur l'ordinateur final.
- Une seconde partition doit exister pour le volume système de BitLocker, la partition en texte au format NTFS contenant au moins 1,5 Go. Microsoft fournit un outil de partitionnement BitLocker.
- BitLocker doit être installé et activé.
- Si TPM doit être utilisé pour l'authentification, TPM doit être initialisé et activé.
- Pour installer le chiffrement basé sur volume de SafeGuard Enterprise, vous devez vérifier qu'aucun volume n'est déjà chiffré avec BitLocker. Dans le cas contraire, le système risque d'être endommagé.

Pour plus d'informations, contactez le support Microsoft. Vous trouverez également des informations sur ces sites Web :

- Informations sur la préparation et sur BitLocker :
  http://technet2.microsoft.com/WindowsVista/en/library/c61f2a12-8ae6-4957-b031-97b4d762cf311033.mspx?mfr=true
- FAQ BitLocker :
  http://technet2.microsoft.com/WindowsVista/en/library/58358421-a7f5-4c97-ab41-2bcc61a58a701033.mspx?mfr=true

11.3 Restrictions

AHCI

Si Intel AHCI (Advanced Host Controller Interface) est utilisé sur l'ordinateur, le disque dur d'amorçage doit être installé dans le slot 0 ou le slot 1. Vous pouvez insérer jusqu'à 32 disques durs. SafeGuard Enterprise ne fonctionne que sur les deux premiers numéros de slot.

Disques dynamiques et GPT

Les disques dynamiques et GPT (GUID Partition Table) ne sont pas pris en charge. Dans ces cas-là, l'installation est interrompue. Si de tels disques sont trouvés sur l'ordinateur ultérieurement, ils ne sont pas pris en charge.

Disques durs SCSI

Le client SafeGuard Enterprise Device Encryption ne prend pas en charge les systèmes équipés de disques durs reliés par un bus SCSI.

Restrictions pour le chiffrement initial des clients SafeGuard Enterprise (gérés)

La configuration initiale des clients SafeGuard Enterprise peut impliquer la création de stratégies de chiffrement pouvant être distribuées aux clients SafeGuard Enterprise sous forme de packages de configuration.

Toutefois, lorsque le client SafeGuard Enterprise ne se connecte pas à un serveur SafeGuard Enterprise juste après l'installation du package de configuration et qu'il est temporairement hors ligne, seules les stratégies de chiffrement présentant les paramètres spécifiques suivants sont immédiatement activées sur le client Enterprise :

- Protection des périphériques basés sur le volume avec la clé machine définie comme clé de chiffrement

Pour que toutes les autres stratégies impliquant le chiffrement à l'aide de clés définies par l'utilisateur soient activées sur le client Enterprise, les packages de configuration correspondants doivent également être réaffectés à l'unité organisationnelle du client Enterprise. Les clés définies par l'utilisateur sont créées uniquement lorsque la connexion entre le client Enterprise et le serveur SafeGuard Enterprise est rétablie.

Cela est dû au fait que la clé machine définie est directement créée sur le client SafeGuard Enterprise lors du premier redémarrage après installation, alors que les clés définies par l'utilisateur ne peuvent être créées sur le client SafeGuard Enterprise qu'une fois que ce dernier a été enregistré sur le serveur SafeGuard Enterprise.

Restrictions pour les clients Sophos SafeGuard (autonomes)

- Les modules suivants ne sont pas pris en charge pour les clients Sophos SafeGuard (autonomes) :
  - Prise en charge de SafeGuard BitLocker
  - Configuration Protection

Restrictions pour la prise en charge de BitLocker

Le package d'installation suivant n'est pas disponible pour les clients SafeGuard Enterprise (gérés) prenant en charge BitLocker :

- SGNClient_withoutDE.msi/SGNClient_withoutDE_x64.msi

11.4 Comptes de service pour tâches de post-installation

Pour éviter que les opérations d'administration sur un ordinateur protégé par SafeGuard Enterprise n'activent l'authentification au démarrage et n'entraînent l'ajout des opérateurs en charge du déploiement comme autant d'utilisateurs possibles de l'ordinateur, SafeGuard Enterprise offre la possibilité de créer des listes de comptes de service pour les ordinateurs finaux. Les utilisateurs figurant dans ces listes sont ainsi traités comme des utilisateurs invités de SafeGuard Enterprise.

Avec les comptes de service, le scénario est le suivant :

- SafeGuard Enterprise est installé sur un ordinateur final.
- Après réinitialisation de l'ordinateur, un opérateur en charge du déploiement figurant sur une liste de comptes de service se connecte (connexion Windows).
- D'après la liste des comptes de service appliqué à l'ordinateur, l'utilisateur est identifié comme un compte de service et par conséquent traité comme un utilisateur invité.
- L'opérateur en charge du déploiement ne sera pas ajouté à l'authentification au démarrage et celle-ci restera inactive. L'utilisateur final peut se connecter et activer l'authentification au démarrage.

Avis : des listes de comptes de service doivent être attribuées dans le premier package de configuration créé pour la configuration des ordinateurs finaux. Pour plus d'informations, consultez l'aide de l'Administrateur.

11.5 Tâches requises pour l'installation centralisée

En tant que responsable de la sécurité, créez un package d'installation comprenant les éléments suivants :

- Package d'installation préparatoire

  Utilisez SGxClientPreinstall.msi. Le package fournit aux ordinateurs finaux la configuration requise pour une installation réussie du logiciel de chiffrement, par exemple le fichier requis DLL MSVCR80.dll, version 8.0.50727.4053.

Avis : si ce package n'est pas installé, l'installation du logiciel de chiffrement est annulée.

- Package d'installation du client SafeGuard Enterprise

  Les packages d'installation du client sont compris sur le CD du produit.
  Les packages d'installation s'appliquent aux clients Enterprise et aux clients autonomes. Pour les clients autonomes, le package Configuration Protection peut cependant ne pas être installé.

Avis : Si vous utilisez le système d'exploitation Windows 7 64 bits ou Windows Vista 64 bits sur les ordinateurs finaux (<nom packaget>_x64.msi), vous pourrez installer la variante 64 bits des packages « client » .msi. Le package 64 bits de SafeGuard Configuration Protection est disponible pour Windows 7 64 bits.

- Package de configuration pour les ordinateurs finaux

  Le package de configuration pour les ordinateurs finaux doit être généré au préalable.
  Des packages de configuration différents doivent être installés pour les ordinateurs finaux gérés et autonomes. Avant d'installer un nouveau package de configuration sur un ordinateur final, n'oubliez pas de désinstaller les packages obsolètes.

- Script avec des commandes d'installation automatique

Vous devez distribuer ce package d'installation aux ordinateurs finaux dans l'ordre spécifié. Pour ce faire, vous pouvez utiliser la commande de Windows Installer, `msiexec`. Les packages sont exécutés sur les ordinateurs finaux. Les ordinateurs finaux sont alors prêts pour l'utilisation de SafeGuard Enterprise.

L'aide de l'utilisateur décrit le comportement des ordinateurs finaux à la première connexion, après l'installation de SafeGuard Enterprise.

11.6 Configuration de l'ordinateur final

Selon la configuration requise, vous devez créer des packages de configuration spécifiques pour l'ordinateur final dans SafeGuard Management Center.

11.6.1 Création d'un package de configuration de client SafeGuard Enterprise (géré)

Pour créer un package de configuration de client SafeGuard Enterprise (géré), procédez comme suit :

1. Démarrez SafeGuard Management Center. Dans le menu **Outils**, sélectionnez **Outil du package de configuration**.
2. Sélectionnez **Créer un package de configuration (géré)**.
   a) Cliquez sur **Ajouter un package de configuration** pour créer le package de configuration du client SafeGuard Enterprise (géré).
   b) Donnez un nom à ce package (MSI).
   c) Attribuez un serveur principal (le serveur secondaire n'est pas absolument indispensable).
   d) Si nécessaire, spécifiez une stratégie créée dans SafeGuard Management Center à appliquer aux ordinateurs finaux. Pour cela,voir *Restrictions pour le chiffrement initial des clients SafeGuard Enterprise (gérés)* à la page 82. Si vous souhaitez utiliser des comptes de service pour les tâches de post-installation sur l'ordinateur, n'oubliez pas d'inclure le paramètre dans ce premier groupe de stratégies. Pour cela, voir *Comptes de service pour tâches de post-installation* à la page 83.
   e) Sélectionnez le mode **Chiffrement du transport** définissant comment chiffrer la connexion entre le client SafeGuard Enterprise et le serveur SafeGuard Enterprise :
   - Chiffrement SafeGuard
   - Chiffrement SSL

     Le protocole SSL présente l'avantage d'être standard et de permettre d'établir une connexion plus rapidement qu'en utilisant le chiffrement de transport SafeGuard.

Remarque : si vous utilisez le chiffrement de transport SSL entre le serveur et le client, vous devez configurer IIS à l'avance de façon appropriée :
- Une autorité de certification doit être installée pour générer des certificats utilisés pour le chiffrement SSL.
- Un certificat doit être généré et le serveur IIS configuré pour utiliser SSL et sélectionner le certificat.

- Le nom du serveur spécifié lors de la configuration du serveur SafeGuard Enterprise doit être identique à celui spécifié dans le certificat SSL. Sinon, le client et le serveur ne peuvent pas communiquer. Un certificat distinct est nécessaire pour chaque serveur SafeGuard Enterprise.
- Si vous utilisez un équilibreur de charge réseau, vérifiez que la plage de ports inclut le port SSL.
Pour plus d'informations, voir *Protection des connexions de transport avec SSL* à la page 11.

f) Spécifiez le chemin de sortie, puis cliquez sur **Créer un package de configuration**. Le fichier SGNClientConfig.msi est créé dans le répertoire spécifié.

Le package de configuration a été créé pour le client SafeGuard Enterprise (géré). Déployez ce package sur l'ordinateur final.

11.6.2 Création du package de configuration d'un client Sophos SafeGuard (autonome)

Pour créer un package de configuration de client Sophos SafeGuard (autonome), procédez comme suit :

1. Dans SafeGuard Management Center, sélectionnez **Outils** > **Outil de package de configuration** dans la barre de menus.
2. Sélectionnez **Créer un package de configuration** (**autonome**) pour une configuration autonome.
   a) Cliquez sur **Ajouter un package de configuration**.
   b) Donnez un nom à ce package (MSI).
   c) Spécifiez un **Groupe de stratégies** qui doit être préalablement créé dans SafeGuard Management Center pour être appliqué aux clients autonomes. Contrairement aux clients Enterprise, vous pouvez appliquer des groupes de stratégies uniquement aux clients autonomes et non des stratégies individuelles. Si vous souhaitez utiliser des comptes de service pour les tâches de post-installation sur l'ordinateur, n'oubliez pas d'inclure le paramètre dans ce premier groupe de stratégies. Pour cela, voir *Comptes de service pour tâches de post-installation* à la page 83.
   d) Pour rendre possible la récupération au niveau des clients autonomes, les données nécessaires doivent être fournies au support. Pour les clients autonomes, ces données sont enregistrées en tant que fichier de récupération spécifique (fichier .xml). Ce fichier est créé lors de la configuration du client autonome. Il contient la clé machine définie, la clé du noyau, une clé de session ainsi qu'une copie du MBR.

e) Dans **Emplacement de sauvegarde de clé**, spécifiez un chemin d'accès réseau partagé ou sélectionnez-le dans la liste déroulante pour stocker ce fichier (.xml), afin qu'il soit accessible au support en cas d'urgence. Entrez le chemin d'accès partagé sous la forme suivante :
`\\networkcomputer\`, par exemple `\\mycompany.edu\`.

Si vous ne spécifiez pas de chemin ici, l'utilisateur devra indiquer l'emplacement de ce fichier à sa première connexion sur l'ordinateur final.

Remarque : veillez à enregistrer le fichier .xml sur un emplacement accessible au support, un chemin d'accès réseau partagé par exemple. Les fichiers peuvent également être fournis au support à l'aide de différents mécanismes. Ce fichier de clés de récupération (.xml) est chiffré par le certificat d'entreprise. Il peut donc être enregistré sur un support externe ou sur le réseau afin d'être fourni au support en cas d'urgence. Il peut également être envoyé par e-mail.

f) Sous **Groupe POA**, vous pouvez sélectionner un groupe de comptes d'accès à l'authentification au démarrage à attribuer à l'ordinateur final. Les comptes d'accès à l'authentification au démarrage permettent d'accéder à des tâches d'administration sur l'ordinateur final une fois l'authentification au démarrage activée. Pour attribuer des comptes d'accès à l'authentification au démarrage, le groupe POA doit avoir été créé au préalable dans la zone **Utilisateurs** de SafeGuard Management Center. Pour plus de détails, consultez l'aide de l'Administrateur.

g) Spécifiez un chemin de sortie pour le package de configuration (fichier .msi).

h) Cliquez sur **Créer un package de configuration**.

Le package de configuration est créé dans le répertoire spécifié. Vous devez maintenant distribuer ce package aux ordinateurs finaux (autonomes) et le déployer sur ces derniers.

11.7 Commande pour l'installation centralisée

Pour l'installation centralisée du logiciel client SafeGuard Enterprise sur les ordinateurs finaux, utilisez le composant « msiexec » de Windows Installer. « msiexec » fait déjà partie de Windows XP, Vista et Windows 7 et exécute automatiquement une installation préconfigurée du client SafeGuard Enterprise. Comme la source et la destination du programme d'installation peuvent également être spécifiées, l'installation standard sur plusieurs ordinateurs finaux existe.

Syntaxe de la ligne de commande

```
msiexec /i <chemin+nom du package msi> /qn ADDLOCAL=ALL | <fonctions
SGN> <paramètre SGN>
```

La syntaxe de la ligne de commande est constituée des éléments suivants :

- **paramètres de Windows Installer**, par exemple, les avertissements des journaux et les messages d'erreur envoyés dans un fichier lors de l'installation ;
- **fonctions de SafeGuard Enterprise** à installer, par exemple, le chiffrement basé sur fichier ;
- **paramètres de SafeGuard Enterprise**, par ex. pour spécifier le répertoire d'installation.

11.7.1 Options de commande

Vous pouvez sélectionner toutes les options disponibles en utilisant msiexec.exe dans l'invite. Les principales options sont décrites ci-dessous.

Option	Description
`/i`	Spécifie qu'il s'agit d'une installation.
`/qn`	Exécute une installation sans interaction de l'utilisateur et n'affiche pas d'interface utilisateur.
`ADDLOCAL=`	Répertorie les fonctions à installer. Si l'option n'est pas spécifiée, toutes les fonctions d'une installation standard sont installées. Pour dresser la liste des fonctions sous ADDLOCAL, gardez à l'esprit les éléments suivants : - Séparez les fonctions à l'aide d'une virgule et non d'un espace. - Respectez la casse. - Si vous sélectionnez une fonction, vous devez également ajouter toutes les fonctions parentes à la ligne de commande.
`ADDLOCAL=ALL`	Installe toutes les fonctions disponibles.
`REBOOT=Force | ReallySuppress`	Force ou supprime une réinitialisation après l'installation. Si rien n'est spécifié, la réinitialisation est forcée après l'installation.
`/L*` <chemin + nom de fichier>	Consigne tous les avertissements et messages d'erreur dans le fichier journal spécifié. Le paramètre `/Le` <chemin + nom de fichier> consigne uniquement les messages d'erreur.
`Installdir=` <répertoire>	Spécifie le répertoire dans lequel installer le client SafeGuard Enterprise. Si aucune valeur n'est spécifiée, le répertoire d'installation par défaut est <SYSTEM>:\PROGRAM FILES\SOPHOS.

11.7.2 Fonctions du client SafeGuard (ADDLOCAL)

Pour une installation centralisée, vous devez définir au préalable les fonctions de SafeGuard Enterprise devant être installées sur les ordinateurs finaux. Les fonctions sont répertoriées après la déclaration de l'option `ADDLOCAL` dans la commande.

Avant cette installation, vous devez décider si vous souhaitez utiliser SafeGuard Enterprise en association avec le chiffrement basé sur volume de BitLocker ou avec le chiffrement de SafeGuard Enterprise dans son intégralité.

Avis : pour installer le chiffrement basé sur volume de SafeGuard Enterprise, vous devez vérifier qu'aucun volume n'est déjà chiffré avec BitLocker. Dans le cas contraire, le système risque d'être endommagé.

Le tableau suivant répertorie les fonctions du client SafeGuard Enterprise que vous pouvez installer de manière centralisée sur les ordinateurs finaux. Si vous sélectionnez une fonction, vous devez également ajouter les fonctions parentes à la ligne de commande.

Fonctions pour SafeGuard Device Encryption

Les fonctions **Client** et **Authentification** doivent être installées par défaut !

Fonctions parentes	Fonction
Client	**Authentification** La fonction **Authentification** et sa fonction parente **Client** doivent être installées par défaut.
Client, Authentification	**CredentialProvider** Vous devez sélectionner cette fonction sur les ordinateurs fonctionnant sous Windows Vista/Windows 7. Elle permet la connexion à l'aide du fournisseur d'informations d'identification.

Fonctions parentes	Fonction
Client	**SecureDataExchange** Avec SecureDataExchange, le chiffrement basé sur fichier de SafeGuard Data Exchange est toujours installé localement et pour les supports amovibles. SafeGuard Data Exchange fournit le chiffrement sécurisé pour les supports amovibles. Les données peuvent être partagées avec d'autres utilisateurs en toute sécurité et facilement. Tous les processus de chiffrement et de déchiffrement sont exécutés de manière transparente et impliquent une interaction utilisateur minimale. Si vous avez installé SafeGuard Data Exchange sur votre ordinateur, SafeGuard Portable l'est également. SafeGuard Portable permet aux données d'être partagées en toute sécurité avec les clients sur lesquels SafeGuard Data Exchange n'est pas installé. SafeGuard Data Exchange peut être installé parallèlement au client BitLocker.
Client, BaseEncryption	**SectorBasedEncryption** Installe le chiffrement basé sur volume de SafeGuard Enterprise avec les fonctions suivantes : ■ Tous les volumes, supports amovibles inclus, peuvent être chiffrés via le chiffrement basé sur volume de SafeGuard Enterprise. ■ Authentification au démarrage (POA) de SafeGuard Enterprise. ■ Récupération de SafeGuard Enterprise avec Challenge/ Réponse. **REMARQUE :** Vous pouvez spécifier SectorBasedEncryption OU BitLockerSupport.

Fonctions parentes	Fonction
Client, BaseEncryption	**BitLockerSupport** Installe la prise en charge de BitLocker pour SafeGuard Enterprise avec les fonctions suivantes : ■ Chiffrement basé sur volume d'initialisation avec BitLocker. ■ Chiffrement d'autres volumes avec BitLocker. ■ Authentification de préinitialisation de BitLocker. ■ Récupération BitLocker **REMARQUE** : vous pouvez spécifier SectorBasedEncryption OU BitLockerSupport. Non disponible pour les clients Sophos SafeGuard autonomes.
Client	**ConfigurationProtection** Protection des ports et gestion des périphériques Pour installer SafeGuard Configuration Protection, vous devez indiquer cette fonction dans la commande msiexec pour le package d'installation du client ET exécuter la procédure d'installation supplémentaire ; voir *Installation de SafeGuard Configuration Protection* à la page 104. Non disponible pour les clients Sophos SafeGuard autonomes.

Fonctions pour SafeGuard Data Exchange

Les fonctions **Client** et **Authentification** doivent être installées par défaut !

Fonctions parentes	Fonction
Client	**Authentification** La fonction **Authentification** et sa fonction parente **Client** doivent être installées par défaut.
Client	**SecureDataExchange** Avec SecureDataExchange, le chiffrement basé sur fichier de SafeGuard Data Exchange est toujours installé localement et pour les supports amovibles. SafeGuard Data Exchange fournit le chiffrement sécurisé pour les supports amovibles. Les données peuvent être partagées avec d'autres utilisateurs en toute sécurité et facilement. Tous les processus de chiffrement et de déchiffrement sont exécutés de manière transparente et impliquent une interaction utilisateur minimale. Si vous avez installé SafeGuard Data Exchange sur votre ordinateur, vous pouvez également utiliser SafeGuard Portable. Le package SafeGuard Data Exchange contient également SafeGuard Portable, qui permet aux données d'être partagées en toute sécurité avec les clients sur lesquels SafeGuard Data Exchange n'est pas installé. SafeGuard Data Exchange peut être installé parallèlement au client BitLocker.
Client	**ConfigurationProtection** Protection des ports et gestion des périphériques Pour utiliser SafeGuard Configuration Protection, vous devez indiquer cette fonction dans la commande msiexec pour le package d'installation du client ET exécuter la procédure d'installation supplémentaire ; voir *Installation de SafeGuard Configuration Protection* à la page 104. Non disponible pour les clients Sophos SafeGuard autonomes.

11.7.3 Exemple de commande pour le chiffrement basé sur fichier et sur volume

La commande indiquée ci-dessous exécute les tâches suivantes :

- ordinateurs finaux disposant de la configuration requise pour une installation réussie du logiciel de chiffrement ;
- authentification au démarrage (POA) de SafeGuard Enterprise pour exécuter l'authentification sur les ordinateurs finaux SafeGuard Enterprise ;
- installation du chiffrement basé sur fichier de SafeGuard Data Exchange en spécifiant `SecureDataExchange` ;
- installation du chiffrement basé sur volume de SafeGuard Enterprise ;
- création d'un fichier journal ;
- et pour finir, exécution du package de configuration du client SafeGuard Enterprise (géré).

EXEMPLE :

```
msiexec /i F:\Software\SGxClientPreinstall.msi /qn /log
I:\Temp\SGxClientPreinstall.log

msiexec /i F:\Software\SGNClient.msi /qn /log I:\Temp\SGNClient.log
ADDLOCAL=Client,Authentication,SecureDataExchange,BaseEncryption,
SectorBasedEncryption

Installdir=C:\Program Files\Sophos\SafeGuard Enterprise

msiexec /i F:\Software\SGNEnterpriseClientConfig.msi /qn /log
I:\Temp\SGNEnterpriseClientConfig.log
```

11.7.4 Exemple de commande pour Windows Vista avec prise en charge de BitLocker

L'exemple de commande exécute les tâches suivantes :

- ordinateurs finaux disposant de la configuration requise pour une installation réussie du logiciel de chiffrement ;
- connexion des utilisateurs à leur PC à l'aide du fournisseur d'informations d'identification Windows Vista ;
- installation du chiffrement basé sur fichier de SafeGuard Data Exchange en spécifiant `SecureDataExchange` ;
- installation de SafeGuard Enterprise prenant en charge BitLocker avec chiffrement basé sur volume de BitLocker ;
- création d'un fichier journal ;
- exécution du package de configuration du client SafeGuard Enterprise (géré).

Remarque : lors de l'installation de SafeGuard Enterprise avec BitLocker, vérifiez que seul le chiffrement basé sur volume de BitLocker est exécuté. N'ajoutez pas le chiffrement basé sur volume de SafeGuard Enterprise à la ligne de commande.

EXEMPLE :

```
msiexec /i F:\Software\SGxClientPreinstall.msi /qn /log
I:\Temp\SGxClientPreinstall.log

msiexec /i F:\Software\SGNClient.msi /qn /log I:\Temp\SGNClient.log
ADDLOCAL=Client,Authentication,CredentialProvider,
SecureDataExchange,BaseEncryption,BitLockerSupport

Installdir=C:\Program Files\Sophos\SafeGuard Enterprise

msiexec /i F:\Software\SGNClientConfig.msi /qn /log
I:\Temp\SGNEnterpriseClientConfig.log
```

11.8 Installation conforme à FIPS

La certification FIPS décrit les conditions de sécurité requises des modules de chiffrement. Par exemple, les organismes publics aux États-Unis et au Canada doivent utiliser des logiciels certifiés conformes à FIPS 140-2 pour les informations de sécurité particulièrement sensibles.

SafeGuard Enterprise utilise des algorithmes certifiés conformes à FIPS pour le chiffrement. En ce qui concerne les algorithmes AES, une nouvelle mise en œuvre est installée par défaut s'ils ne sont pas certifiés conformes à FIPS.

Pour utiliser la variante certifiée conforme à FIPS d'un algorithme AES, définissez la propriété FIPS_AES sur 1 lors de l'installation d'un client SafeGuard Enterprise.

Deux méthodes sont possibles :

- Ajoutez la propriété au script de ligne de commande :

  ```
  msiexec /i F:\Software\SGNClient.msi FIPS_AES=1
  ```

- Procédez à une transformation.

12 Configuration locale des ordinateurs finaux

Ce chapitre décrit l'installation du logiciel de chiffrement en local sur l'ordinateur final. Les étapes requises pour les clients SafeGuard Enterprise avec Windows Vista BitLocker sont également décrites.

Pour plus d'informations sur les packages d'installation et de configuration des clients, voir *Configurations de SafeGuard pour les ordinateurs finaux* à la page 72.

Avant l'installation, vous devez décider si vous souhaitez utiliser SafeGuard Enterprise en association avec le chiffrement basé sur volume de BitLocker ou avec le chiffrement de SafeGuard Enterprise.

Avis : pour installer le chiffrement basé sur volume de SafeGuard Enterprise, vous devez vérifier qu'aucun volume n'est déjà chiffré avec BitLocker. Dans le cas contraire, le système risque d'être endommagé.

12.1 Conditions préalables

Pour prendre connaissance des conditions préalables, voir *Conditions préalables générales* à la page 80. Pour connaître les conditions préalables spéciales pour la prise en charge de Windows Vista BitLocker, voir *Conditions préalables pour BitLocker* à la page 81.

12.2 Installation du logiciel de chiffrement sur les ordinateurs locaux

Ce chapitre s'applique aux clients SafeGuard Enterprise (gérés) et aux clients Sophos SafeGuard (autonomes). La procédure d'installation est identique sauf que vous créez un package de configuration différent pour chacun. Avant de procéder à l'installation, décidez des fonctions de SafeGuard Enterprise à utiliser.

12.2.1 Poursuite de l'installation

1. Démarrez le package d'installation préparatoire SGxClientPreinstall.msi depuis le CD du produit pour fournir aux ordinateurs finaux la configuration requise pour une installation réussie du logiciel de chiffrement, notamment les fichiers DLL adéquats.

Avis : vous pouvez également installer vcredist_x86.exe, à télécharger à l'adresse suivante : *http://www.microsoft.com/downloads/details.aspx?FamilyID=766a6af7-ec73-40ff-b072-9112bab119c2* ou vérifier que le fichier MSVCR80.dll, version 8.0.50727.4053 est présent dans le dossier Windows\WinSxS de l'ordinateur.

2. Démarrez le package d'installation client approprié à partir du CD du produit.

3. Acceptez les valeurs par défaut des boîtes de dialogue suivantes.

4. Le cas échéant, sélectionnez le type d'installation et activez les fonctions selon vos besoins. Pour cela, voir *Sélection de fonctions* à la page 98.
5. Sélectionnez un chemin d'installation. Le chemin d'installation par défaut est :

   ```
   C:\Program Files\Sophos\SafeGuard Enterprise
   ```

6. Confirmez la réussite de l'installation.

12.2.2 Création du package de configuration

1. Configurez l'ordinateur final en créant un package de configuration dans SafeGuard Management Center.
   - Pour créer une configuration de client SafeGuard Enterprise (géré), voir *Création d'un package de configuration de client SafeGuard Enterprise (géré)* à la page 85.
   - Pour créer une configuration de client Sophos SafeGuard (autonome), voir *Création du package de configuration d'un client Sophos SafeGuard (autonome)* à la page 86.
2. Distribuez le package de configuration aux ordinateurs finaux.
3. Installez le package de configuration sur l'ordinateur final.

Le logiciel client est désormais entièrement installé.

L'aide de l'utilisateur décrit le comportement des ordinateurs à la première connexion, après l'installation de SafeGuard Enterprise.

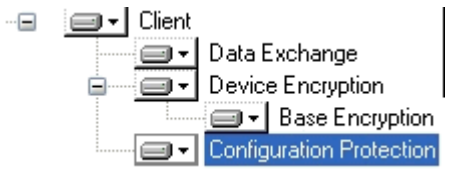
12.3 Sélection de fonctions

Lorsque SafeGuard Enterprise est en cours d'installation sur l'ordinateur, des fonctions facultatives vous sont proposées, en fonction du système d'exploitation et du package d'installation. Pour plus d'informations sur les fonctions, voir *Fonctions du client SafeGuard (ADDLOCAL)* à la page 90.

1. Cliquez sur les fonctions pour les sélectionner.
2. Désactivez les fonctions que vous ne souhaitez pas installer.
3. Poursuivez l'installation.

12.3.1 Fonctions du client pour Windows XP

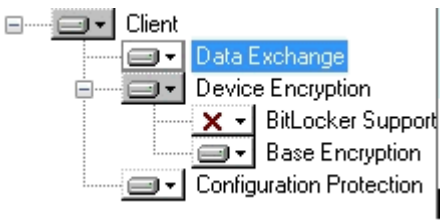
L'illustration indique la sélection des fonctions pour le package d'installation **SGNClient.msi**.



- Chiffrement basé sur fichier de SafeGuard Data Exchange : fonction **Data Exchange** activée.
- Chiffrement basé sur volume : Fonctions **Device Encryption** > **Base Encryption** activées.
- Configuration Protection : fonction **Configuration Protection** activée. Pour prendre connaissance des autres étapes requises pour l'installation de ce module, voir *Installation de SafeGuard Configuration Protection* à la page 104.
  Cette fonction ne peut pas être installée pour les clients autonomes Sophos SafeGuard.

12.3.2 Fonctions du client pour Windows Vista sans prise en charge de BitLocker

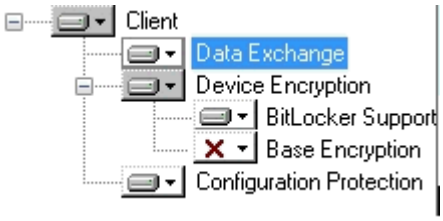
L'illustration indique la sélection des fonctions pour le package d'installation **SGNClient.msi**.



- Chiffrement basé sur fichier de SafeGuard Data Exchange : fonction **Data Exchange** activée.
- Chiffrement basé sur volume de SafeGuard Enterprise :
  - Fonctions **Device Encryption** > **Base Encryption** activées.
  - Fonctions **Device Encryption** > **Prise en charge de BitLocker** désactivées.
- Configuration Protection : fonction **Configuration Protection** activée. Pour prendre connaissance des autres étapes requises pour l'installation de ce module, voir *Installation de SafeGuard Configuration Protection* à la page 104.
  Cette fonction ne peut pas être installée pour les clients autonomes Sophos SafeGuard.

12.3.3 Fonctions du client pour Windows Vista avec prise en charge de BitLocker

L'illustration indique la sélection des fonctions pour le package d'installation **SGNClient.msi**. Pour les clients Sophos SafeGuard autonomes, la prise en charge BitLocker et Configuration Protection ne peuvent pas être installés.



- Chiffrement basé sur fichier de SafeGuard Data Exchange : **Data Exchange** activée.
- Chiffrement basé sur volume de BitLocker :
  - Fonctions **Device Encryption** > **Prise en charge de BitLocker** activées.
  - Fonctions **Device Encryption** > **Base Encryption** désactivées.
- Configuration Protection : fonction **Configuration Protection** activée. Pour prendre connaissance des autres étapes requises pour l'installation de ce module, voir *Installation de SafeGuard Configuration Protection* à la page 104.

13 Installation du logiciel client SafeGuard Enterprise sur les ordinateurs disposant de plusieurs systèmes d'exploitation

Le logiciel client SafeGuard Enterprise peut être installé sur un ordinateur afin d'en protéger les données si plusieurs systèmes d'exploitation sont installés sur différents volumes du disque dur.

SafeGuard Enterprise propose un système d'exécution. Le client d'exécution SafeGuard Enterprise permet les opérations suivantes lorsqu'il est installé sur des volumes disposant d'une installation supplémentaire de Windows :

- L'installation Windows résidant sur ces volumes peut être initialisée correctement via un gestionnaire d'initialisation.
- Vous pouvez accéder aux partitions des volumes chiffrés avec une clé machine définie lors d'une installation complète du client SafeGuard Enterprise.

13.1 Conditions requises et restrictions

Notez les éléments suivants :

- Le client d'exécution SafeGuard Enterprise ne fournit aucune fonction ou fonctionnalité spécifique au client SafeGuard Enterprise.
- Le client d'exécution SafeGuard Enterprise prend en charge uniquement les systèmes d'exploitation également pris en charge par le client SafeGuard Enterprise.
- Le bon fonctionnement des claviers USB peut être limité.
- Seuls les gestionnaires d'initialisation activés à la suite d'une authentification au démarrage sont pris en charge.
- La prise en charge des gestionnaires d'amorçage tiers n'est pas garantie. Nous recommandons d'utiliser les gestionnaires d'initialisation de Windows.
- Le client d'exécution SafeGuard Enterprise ne peut pas être mis à jour vers un client SafeGuard Enterprise complet.
- Ce scénario s'applique aux clients SafeGuard Enterprise et aux clients Sophos SafeGuard autonomes.
- Le package d'installation du client d'exécution doit être installé avant la version complète du package d'installation du client SafeGuard Enterprise.
- Seuls les volumes chiffrés avec la clé machine définie de SafeGuard Enterprise sont accessibles.

13.2 Préparations

Pour configurer le client d'exécution SafeGuard Enterprise, effectuez les préparatifs suivants dans l'ordre indiqué :

1. Assurez-vous que les volumes sur lesquels le client d'exécution SafeGuard Enterprise est exécuté sont visibles au moment de l'installation et peuvent porter leur nom Windows (par exemple C:).

2. Choisissez les volumes du disque dur sur lesquels installer le **client d'exécution SafeGuard Enterprise**. Dans SafeGuard Enterprise, ces volumes sont définis en tant qu'installations **secondaires** de Windows. Il peut exister plusieurs installations secondaires de Windows.

   Vous pouvez installer l'un des packages d'installation suivants à partir du CD du produit :

   - SGNClientRuntime.msi/SGNClientRuntime_x64.msi

3. Choisissez le volume du disque dur sur lequel installer la version complète du **client SafeGuard Enterprise**. Dans SafeGuard Enterprise, ce volume est défini en tant qu'installation **primaire** de Windows. Il ne peut exister qu'une seule installation primaire de Windows.

   Vous pouvez installer l'un des packages d'installation suivants à partir du CD du produit :

   - SGNClient.msi/SGNClient_x64.msi

   Vous pouvez installer ainsi que SGN_CP_Client.msi ou SGN_CP_Client_x64.msi, disponible pour Windows 7 64 bits.

13.3 Configuration du client d'exécution SafeGuard Enterprise

Veuillez procéder comme suit :

1. Sélectionnez les volumes secondaires requis du disque dur sur lesquels installer le client d'exécution SafeGuard Enterprise.

2. Initialisez l'installation secondaire de Windows sur le volume sélectionné.

3. Installez le package d‘installation client d'exécution sur le volume sélectionné.

4. Confirmez les valeurs par défaut de la boîte de dialogue suivante du programme d'installation. Aucune sélection de fonction en particulier n'est nécessaire.

5. Sélectionnez un dossier d'installation du client d'exécution.

6. Confirmez pour terminer l'installation du client d'exécution.

7. Sélectionnez le volume primaire du disque dur sur lequel installer le client SafeGuard Enterprise.

8. Initialisez l'installation primaire de Windows sur le volume sélectionné.
9. Installez le package d'installation préparatoire SGxClientPreinstall.msi pour fournir aux ordinateurs finaux la configuration requise pour une installation réussie du logiciel de chiffrement.
10. Installez le package d'installation du client SafeGuard Enterprise sur le volume sélectionné.
11. Créez et déployez les packages de configuration pour les clients Enterprise (gérés) ou autonomes, le cas échéant.
12. Chiffrez les volumes à l'aide de la clé machine définie.

13.4 Initialisation à partir d'un volume secondaire via un gestionnaire d'initialisation

1. Démarrez l'ordinateur.
2. Connectez-vous à l'authentification au démarrage avec vos informations d'identification.
3. Démarrez le gestionnaire d'initialisation et sélectionnez le volume secondaire requis en tant que volume d'initialisation.
4. Réinitialisez l'ordinateur à partir de ce volume.

Vous pouvez accéder à chacun des volumes chiffrés avec la clé machine définie.

14 Installation de SafeGuard Configuration Protection

SafeGuard Configuration Protection permet de définir les interfaces et les périphériques à autoriser sur les ordinateurs finaux. Ce module empêche l'introduction de programmes malveillants, ainsi que les exportations de données via des canaux non désirés tels que les réseaux locaux sans fil (WLAN). Il peut également détecter et bloquer les matériels nuisibles tels que les enregistreurs de frappe.

14.1 Conditions préalables et restrictions

- Pour installer SafeGuard Configuration Protection sur un système d'exploitation Windows 7 64 bits, vouz pourrez utiliser les variantes 64 bits des packages d'installation « client » .
- SafeGuard Configuration Protection est seulement disponible pour les clients SafeGuard Enterprise (gérés). SafeGuard Configuration Protection n'est pas pris en charge pour les clients Sophos SafeGuard autonomes.
- Vous devez installer .NET version 2.0.

14.2 Flux de travail

Pour installer SafeGuard Configuration Protection sur les ordinateurs finaux, vous devez exécuter un package d'installation distinct après avoir installé le package d'installation du client SafeGuard Enterprise. Les packages d'installation requis se trouvent sur le CD du produit.

Pour installer SafeGuard Configuration Protection sur un système d'exploitation Windows 7 64 bits, vouz pourrez utiliser les variantes 64 bits des packages d'installation « client » .

1. Installez le package d'installation préparatoire SGxPreinstall.msi.
2. Installez un des packages d'installation du client SafeGuard Enterprise suivants:
   - SGNClient.msi/SGNClient_x64.msi
   - SGNClient_withoutDE.msi/SGNClient_withoutDE_x64.msi
3. Installez SafeGuard Configuration Protection :
   - SGN_CP_Client.msi/SGN_CP_Client_x64.msi
4. Générez et installez le package de configuration du client SafeGuard Enterprise.

14.3 Commande pour l'installation centralisée

Pour l'installation centralisée de SafeGuard Configuration Protection sur les ordinateurs finaux, utilisez le composant « msiexec » de Windows Installer.

Syntaxe de la ligne de commande

```
msiexec /i SGN_CP_Client.msi /quiet /norestart
```

14.4 Exemple de commande pour SafeGuard Configuration Protection avec SafeGuard Device Encryption

La commande msiexec doit être exécutée dans l'ordre spécifié dans l'exemple. Dans cet exemple, les événements suivants ont lieu :

- Les ordinateurs finaux disposent de la configuration requise pour une installation réussie du logiciel de chiffrement.
- Le chiffrement basé sur volume de SafeGuard Device Encryption est installé.
- SafeGuard Configuration Protection doit être répertorié comme fonction pour le package d'installation du client SafeGuard Device Encryption.
- Pour initier l'installation du module SafeGuard Configuration Protection, vous devez ajouter un package d'installation distinct en spécifiant une autre commande msiexec.
- Un fichier journal est créé.
- Pour finir, le package de configuration du client, SGNEnterpriseClientConfig.msi, est exécuté.

EXEMPLE :

```
msiexec /i F:\Software\SGxClientPreinstall.msi /qn /log
I:\Temp\SGxClientPreinstall.log


msiexec /i F:\Software\SGNClient.msi /qn /log I:\Temp\SGNClient.log
ADDLOCAL=Client,Authentication,BaseEncryption,SectorBasedEncryption,Co
nfigurationProtection
Installdir=C:\Program Files\Sophos\SafeGuard Enterprise


msiexec /i F:\Software\SGN_CP_Client.msi /quiet /norestart


msiexec /i F:\Software\SGNEnterpriseClientConfig.msi /qn
/log I:\Temp\SGNEnterpriseClientConfig.log
```

14.5 Exemple de commande pour SafeGuard Configuration Protection avec SafeGuard Data Exchange

La commande msiexec doit être exécutée dans l'ordre spécifié dans l'exemple. Dans cet exemple, les événements suivants ont lieu :

- Les ordinateurs finaux disposent de la configuration requise pour une installation réussie du logiciel de chiffrement.
- Le chiffrement basé sur fichier de SafeGuard Data Exchange est installé.
- SafeGuard Configuration Protection doit être répertorié comme fonction pour le package d'installation du client SafeGurd Data Exchange.
- Pour initier l'installation du module SafeGuard Configuration Protection, vous devez ajouter un package d'installation distinct en spécifiant une autre commande msiexec.
- Un fichier journal est créé.
- Pour finir, le package de configuration SGNEnterpriseClientConfig.msi est exécuté.

EXEMPLE :

```
msiexec /i F:\Software\SGxClientPreinstall.msi /qn /log
I:\Temp\SGxClientPreinstall.log

msiexec /i F:\Software\SGNClient_withoutDE.msi /qn /log
I:\Temp\SGNClient.log
ADDLOCAL=Client,Authentication,SecureDataExchange,
         ConfigurationProtection
Installdir=C:\Program Files\Sophos\SafeGuard Enterprise

msiexec /i F:\Software\SGN_CP_Client.msi /quiet /norestart

msiexec /i F:\Software\SGNEnterpriseClientConfig.msi /qn
        /log I:\Temp\SGNEnterpriseClientConfig.log
```

14.6 Installation locale

Pour installer SafeGuard Enterprise Configuration Protection avec succès, respectez l'ordre d'installation suivant :

1. Démarrez le package d'installation préparatoire SGxClientPreinstall.msi depuis le CD du produit pour fournir aux ordinateurs finaux la configuration requise pour une installation réussie du logiciel de chiffrement.
2. Installez l'un des packages d'installation suivants du client SafeGuard Enterprise sur l'ordinateur final. Pour installer SafeGuard Configuration Protection sur un système d'exploitation Windows 7 64 bits, vouz pourrez utiliser les variantes 64 bits des packages d'installation « client » .
   - SGNClient.msi/SGNClient_x64.msi
   - SGNClient_withoutDE.msi/SGNClient_withoutDE_x64.msi
3. Lorsque vous êtes invité à sélectionner les fonctions requises, veillez à activer la fonction Configuration Protection.
4. Installez ensuite le packages d'installation du client SafeGuard Configuration Protection:
   - SGN_CP_Client.msi / SGN_CP_Client_x64.msi (disponible pour Windows 7 64 bits.)

Avis : Pour garantir l'installation du module Configuration Protection dans le répertoire SafeGuard Enterprise, vous devez le remplacer par
`C:\Program Files\Sophos\SafeGuard Enterprise\`

5. Nous recommandons de redémarrer l'ordinateur final. Néanmoins, si le package de configuration du client est directement installé après, le redémarrage peut être différé.
6. Générez et installez le package de configuration du client SafeGuard Enterprise (géré), SGNEnterpriseClientConfig.msi.
7. Redémarrez l'ordinateur.

SafeGuard Configuration Protection est installé sur l'ordinateur final.

14.7 Désinstallation de SafeGuard Configuration Protection

Pour désinstaller SafeGuard Configuration Protection, exécutez les tâches en respectant l'ordre indiqué :

1. Désinstallez le package de configuration du client correspondant.
2. Exécutez le package d'installation du client SafeGuard Enterprise sur l'ordinateur. Il peut s'agir du package SGNClient.msi ou du package SGNClient_withoutDE.msi ou la variante 64 bits des packages.
3. Dans l'assistant d'installation, sélectionnez l'option **Modifier**.
4. Désactivez la fonction **Configuration Protection**.
5. Lorsque la désinstallation est terminée, ne redémarrez pas l'ordinateur !
6. Désinstallez SGN_CP_Client.msi./SGN_CP_Client_x64.msi.
7. Redémarrez l'ordinateur.

SafeGuard Configuration Protection a été supprimé de l'ordinateur final.

14.8 Mise à jour de SafeGuard Configuration Protection

Pour mettre à jour SafeGuard Configuration Protection vers la version la plus récente, exécutez les tâches en respectant l'ordre indiqué :

1. Démarrez le package d'installation préparatoire SGxClientPreinstall.msi depuis le CD du produit pour fournir aux ordinateurs finaux la configuration requise pour une installation réussie du logiciel de chiffrement.
2. Mettez à jour le package d'installation du client SafeGuard Enterprise sur l'ordinateur vers la version en cours. Pour cela, voir *Mise à jour des ordinateurs finaux protégés par SafeGuard Enterprise* à la page 114.

Avis : ne réamorcez pas l'ordinateur après cela.

3. Désinstallez le module client SafeGuard Configuration Protection client actuellement installé. Pour cela, voir *Désinstallation de SafeGuard Configuration Protection* à la page 108.
4. Installez le tout dernier module client SafeGuard Configuration Protection de zéro. Pour cela, voir *Installation locale* à la page 107.

15 Empêchement de la désinstallation sur le PC de l'utilisateur

Pour renforcer la protection des PC d'utilisateur, vous pouvez empêcher la désinstallation locale de SafeGuard Enterprise via une stratégie de machine centralisée. Si ce type de stratégie est appliqué au PC de l'utilisateur, SafeGuard Enterprise ne peut être désinstallé qu'une fois la stratégie attribuée. Sinon, la désinstallation est annulée et la tentative non autorisée est consignée. Consultez l'aide administrateur de SafeGuard Enterprise pour plus de détails sur les stratégies.

Remarque : Si vous utilisez une version de démonstration, vous ne devez pas activer ni désactiver ce paramètre de stratégie avant l'expiration de cette version afin de faciliter la désinstallation.

16 Mise à jour de SafeGuard Enterprise

Si vous avez déjà installé une version précédente de SafeGuard Enterprise, vous pouvez mettre à jour ce logiciel en installant la toute dernière version. La mise à jour directe vers SafeGuard Enterprise 5.50 est prise en charge pour SafeGuard Enterprise 5.35 et les versions ultérieures. Si vous procédez depuis des versions antérieures, vous devez commencer par effectuer une mise à jour vers SafeGuard Enterprise 5.40.

À l'exception de la base de données SafeGuard Enterprise, les mises à jour du serveur SafeGuard Enterprise, de Management Center et de l'ordinateur final constituent une nouvelle installation.

Depuis SafeGuard Enterprise 5.30 et versions supérieures, l'importation d'un fichier de licence valide est requise pour couvrir tous les clients déployés. Si le nombre de licences est dépassé, le transport de stratégie est bloqué après la mise à jour du client. Contactez au préalable votre partenaire commercial pour lui demander un fichier de licence.

Remarque : il est essentiel de mettre à jour les composants dans l'ordre indiqué ci-dessous. Les mises à jour d'une version précédente vers la version actuelle de SafeGuard Enterprise n'aboutissent que si vous respectez cet ordre. La mise à jour des composants de SafeGuard Enterprise est prise en charge pour SafeGuard Enterprise 5.30 ou version ultérieure.

SafeGuard Enterprise

1. Base de données SafeGuard Enterprise
2. Serveur SafeGuard Enterprise
3. SafeGuard Management Center
4. Ordinateurs finaux protégés par SafeGuard Enterprise

16.1 Mise à jour de la base de données SafeGuard Enterprise

Plusieurs scripts SQL sont fournis sur le CD du produit pour la mise à jour de la base de données SafeGuard Enterprise.

Conditions préalables

- Une base de données SafeGuard Enterprise version 5.20 ou supérieure doit être installée.
- Les scripts SQL à exécuter doivent être présents sur l'ordinateur hébergeant la base de données.
- Vous devez posséder les droits d'administrateur Windows sur le serveur de base de données.
- Sauvegardez la base de données SafeGuard Enterprise avant de procéder à la mise à jour.

Mise à jour de la base de données

1. Déconnectez tous les serveurs SafeGuard Enterprise (serveurs IIS) connectés à la base de données SafeGuard Enterprise concernée.
2. Fermez toutes les instances ouvertes de SafeGuard Management Center connectées à la base de données SafeGuard Enterprise concernée.
3. Définissez la base de données SafeGuard Enterprise en mode SINGLE_USER pour l'exécution des scripts SQL afin de disposer d'un accès exclusif à la base de données.
4. La base de données doit être migrée version par version vers la version actuelle. En fonction de la version installée, démarrez les scripts SQL suivants dans cet ordre :
   a) 5.20 > 5.3x : exécuter `MigrateSGN520_SGN530.sql` ou `MigrateSGN520_SGN535.sql`
   Avis : les stratégies SafeGuard Enterprise existantes sont modifiées car la structure de la stratégie a changé entre la version 5.20 et la version 5.3x.
   b) 5.3x > 5.35 : exécuter `MigrateSGN530_SGN535.sql`
   c) 5.30 > 5.40 : exécuter `MigrateSGN530_SGN540.sql`
   d) 5.35 > 5.40 : exécuter `MigrateSGN535_SGN540.sql`
   e) 5.40 > 5.50 : exécuter `MigrateSGN540_SGN550.sql`
5. Redéfinissez la base de données SafeGuard Enterprise en mode MULTI_USER.

Les sommes de contrôle cryptographiques de certains tableaux peuvent ne plus être correctes après la mise à jour de la base de données. Des messages d'erreur s'affichent alors au démarrage de SafeGuard Management Center. Vous pouvez réparer les tableaux dans la boîte de dialogue correspondante. La dernière version de la base de données SafeGuard Enterprise peut ensuite être utilisée.

16.2 Mise à jour des bases de données dupliquées SafeGuard Enterprise

Lorsque la base de données SafeGuard Enterprise est à mettre à jour vers une version ultérieure et que les bases de données sont en cours d'utilisation, il est recommandé de désinstaller les bases de données dupliquées avant de démarrer la mise à jour sur la base de données principale.

La mise à jour de la base de données SafeGuard Enterprise nécessite l'exécution de scripts de migration SQL spécifiques qui risquent d'entrer en conflit avec les bases de données dupliquées.

1. Désinstallez les bases de données dupliquées.
2. Exécutez les scripts de migration SQL sur la base de données principale. Vous pouvez les trouver dans le dossier Outils du CD du produit (voir *Mise à jour de la base de données SafeGuard Enterprise* à la page 111).
3. Configurez à nouveau les bases de données dupliquées.

16.3 Mise à jour du serveur SafeGuard Enterprise

Conditions préalables

- La base de données SafeGuard Enterprise a déjà été mise à jour vers la dernière version.
- Un serveur SafeGuard Enterprise 5.35 ou version ultérieure doit être installé. Les versions antérieures à la version 5.35 doivent être mises à jour en premier vers SafeGuard Enterprise Server 5.40.
- Vous devez disposer des droits d'administrateur Windows.
- Vous devez avoir mis à niveau ASP.NET vers la version 2.0.

Poursuite de la mise à jour

Réinstallez le serveur. Pour cela, voir *Installation du serveur SafeGuard Enterprise* à la page 52. Lorsque la mise à jour a été effectuée, le serveur redémarre automatiquement et redevient utilisable.

16.4 Mise à jour de SafeGuard Management Center

Conditions préalables

- SafeGuard Management Center 5.35 ou version ultérieure doit être installé. Les versions antérieures à la version 5.35 doivent être mises à jour en premier vers SafeGuard Management Center 5.40.
- La base de données SafeGuard Enterprise et le serveur SafeGuard Enterprise ont déjà été mis à jour vers la dernière version.
- NET Framework 3.0 Service Pack 1 doit être installé pour réussir la mise à jour vers la dernière version.
- Vous devez avoir mis à niveau ASP.NET vers la version 2.0.
- Vous devez disposer des droits d'administrateur Windows.
- Vous devez disposer d'un fichier de licence valide. Contactez au préalable votre partenaire commercial pour lui en demander un.

Poursuite de la mise à jour

1. Réinstallez Management Center (voir *Configuration du serveur SafeGuard Enterprise* à la page 43) avec les fonctionnalités requises.
2. Importez le fichier de licence.
3. Démarrez SafeGuard Management Center. Le comportement de SafeGuard Management Center au premier démarrage après mise à jour dépend de l'installation ou non de la fonctionnalité Multi Tenancy.
   - La fonctionnalité Multi Tenancy n'a pas été installée : vous êtes invité à saisir les informations d'identification du responsable de la sécurité.
   - La fonctionnalité Multi Tenancy a été installée : l'assistant de configuration de SafeGuard Management Center démarre et vous invite à sélectionner la base de données à utiliser. L'assistant présélectionne par défaut une base de données utilisée précédemment. Sélectionnez la base de données requises et terminez la configuration avec l'assistant.

Avis :

- Le fichier de configuration par défaut de SafeGuard Management Center a été déplacé et renommé. Vous le trouverez à l'emplacement suivant :
  - **Windows XP :** <CSIDL_LOCAL_APPDATA>\Sophos\SafeGuard Enterprise\Configuration\<hash>.xml
  - **Windows Vista :** C:\Users\<nom utilisateur>\AppData\Local\Sophos\SafeGuard Enterprise\Configuration\FE2E60C269D115B176D195AB3ABF8324.xml

- API de script : Du fait du nouveau nom et du nouvel emplacement de stockage attribué au fichier de configuration par défaut, assurez-vous que le chemin et le nom du fichier renvoient effectivement au nouvel emplacement lorsque vous utilisez la méthode suivante avec le paramètre confFilePathName :

  `AuthenticateOfficer (string OfficerName, string PinOrPassword, string confFilePathName).`

- Si la fonctionnalité Multi Tenancy est installée avec la mise à jour, l'assistant de configuration de SafeGuard Management démarre à la suite de la première mise à jour. L'assistant présélectionne par défaut une configuration de base de données utilisée précédemment.
- Si la fonctionnalité Multi Tenancy n'est pas installée, la dernière configuration utilisée est appliquée à SafeGuard Management Center. Après réinstallation de la fonctionnalité Multi Tenancy, cette configuration sera présélectionnée.
- Notez que les stratégies SafeGuard Enterprise existantes peuvent être modifiées en raison du changement de structure des stratégies par rapport à SafeGuard Enterprise version 5.30 et supérieures.

16.5 Mise à jour des ordinateurs finaux protégés par SafeGuard Enterprise

Cette section s'applique aux ordinateurs finaux gérés et autonomes.

Le serveur SafeGuard Enterprise et SafeGuard Management Center 5.50 peuvent gérer des clients SafeGuard Enterprise 5.35 et versions ultérieures (gérés et autonomes).

Conditions préalables

- Un logiciel client SafeGuard Enterprise 5.35 ou version ultérieure doit être installé. Les versions antérieures à la version 5.35 doivent être mises à jour en premier vers le client SafeGuard Enterprise 5.40.
- La base de données SafeGuard Enterprise, le serveur SafeGuard Enterprise et SafeGuard Management Center ont déjà été mis à jour vers la dernière version.
- Vous devez disposer des droits d'administrateur Windows.

Avis :

- Recherchez sur votre réseau et sur vos ordinateurs la présence de packages de configuration client obsolètes ou inutilisés, puis supprimez-les pour des raisons de sécurité.

Poursuite de la mise à jour

Vous devez mettre à jour le client SafeGuard Enterprise version par version jusqu'à la version 5.50.

1. Démarrez le package d'installation préparatoire SGxClientPreinstall.msi depuis le dossier de mise à disposition de votre logiciel pour fournir aux ordinateurs finaux la configuration requise pour une installation réussie du logiciel de chiffrement.
2. Installez le package d'installation du client concerné. Pour cela, voir *Installation centralisée des ordinateurs finaux* à la page 80 ou voir *Configuration locale des ordinateurs finaux* à la page 97.

Windows Installer reconnaît les modules déjà installés et n'installe que ces modules. Si l'authentification au démarrage est installée, un noyau POA à jour sera également disponible après la mise à jour (stratégies, clés, etc.). Le client SafeGuard Enterprise redémarre automatiquement.

Avis : si la configuration du client est restée inchangée, il est inutile de créer et d'installer un nouveau package de configuration client. Toutefois, pour des raisons de sécurité, nous vous recommandons de supprimer tous les packages de configuration client obsolètes ou inutilisés.

Il n'est pas utile de créer et de réinstaller un nouveau package de configuration de client si aucune modification n'a été apportée à la configuration. Si vous créez un nouveau package de configuration client, n'oubliez pas de supprimer celui qui devient alors obsolète.

Si vous tentez d'installer un package de configuration client plus ancien sur une version plus récente, l'installation échoue et un message d'avertissement s'affiche.

16.5.1 Mise à niveau des clients Sophos SafeGuard (autonomes) avec le chiffrement basé sur volume

Si vous souhaitez améliorer un ordinateur final autonome (client Sophos SafeGuard autonome) sur lequel seul le module SafeGuard Data Exchange avec chiffrement basé sur fichier est installé en lui ajoutant le chiffrement basé sur volume, vous devez exécuter les étapes suivantes. Ces étapes sont nécessaires pour garantir une authentification au démarrage sécurisée et correcte.

1. Désinstallez le package d'installation de SafeGuard Data Exchange, (SGNClient_withoutDE.msi/SGNClient_withoutDE_x64.msi.)
2. Désinstallez le package de configuration du client Sophos SafeGuard (autonome).
3. Installez le package d'installation du client avec le chiffrement basé sur volume (SGNClient.msi/ SGNClient_x64.msi) en sélectionnant les fonctions Device Encryption et Data Exchange.
4. Générez et installez un nouveau package de configuration du client Sophos SafeGuard (autonome).

Le fichier de clés de récupération ainsi que les clés locales créés lors de l'installation du package Data Exchange ne sont pas supprimés, mais toujours disponibles.

16.6 Mise à niveau des ordinateurs autonomes en ordinateurs gérés

Vous pouvez mettre à niveau des ordinateurs finaux dotés d'une configuration de client Sophos SafeGuard (autonome) pour en faire des ordinateurs dotés d'une configuration de client SafeGuard Enterprise (géré). Les ordinateurs finaux sont ainsi définis dans SafeGuard Management Center en tant qu'objets pouvant être gérés et disposant d'une connexion avec le serveur SafeGuard Enterprise.

Avis : il n'est pas conseillé d'effectuer la procédure inverse, c'est-à-dire de migrer un client SafeGuard Enterprise vers un client autonome. Pour ce faire, vous devez complètement réinstaller SafeGuard Enterprise avec la configuration autonome sur l'ordinateur final.

Conditions préalables

- SafeGuard Policy Editor a été mis à niveau vers SafeGuard Management Center.
- Vous n'avez pas besoin de désinstaller le package d'installation du client.
- Veillez à sauvegarder l'ordinateur final avant de procéder à la mise à niveau.
- Vous devez disposer des droits d'administrateur Windows.

Poursuite de la mise à niveau

Pour la mise à niveau, il vous suffit de créer le package de configuration correspondant requis pour les ordinateurs gérés et de l'attribuer aux ordinateurs finaux :

1. Créez le package de configuration pour le client SafeGuard Enterprise (géré) dans SafeGuard Management Center via **Outils** > **Outil de package de configuration** > **Créer un package de configuration** (**géré**).
2. Attribuez ce package à l'ordinateur final via une stratégie de groupe.

Avis : lors de la mise à niveau, tous les utilisateurs et tous les certificats sont supprimés et l'authentification au démarrage est désactivée, car l'attribution utilisateur-ordinateur n'est pas mise à niveau. Après la mise à niveau, les ordinateurs finaux ne sont donc plus protégés !

3. Réinitialisez l'ordinateur deux fois après la mise à niveau : la première connexion est toujours effectuée via l'ouverture de session automatique de Windows. De nouvelles clés et de nouveaux certificats sont attribués à l'utilisateur. Par conséquent, il ne peut se connecter à l'authentification au démarrage que lors de la seconde réinitialisation. C'est seulement après la seconde réinitialisation que les ordinateurs finaux sont à nouveau protégés.

Le client Sophos SafeGuard (autonome) est maintenant devenu un client SafeGuard Enterprise (géré).

16.7 Mise à jour de SafeGuard Configuration Protection

Pour mettre à jour le module client SafeGuard Configuration Protection, voir *Mise à jour de SafeGuard Configuration Protection* à la page 108.

17 Mise à niveau de Sophos SafeGuard 5.5x vers SafeGuard Enterprise

Sophos SafeGuard 5.5x est composé des produits suivants :

- Sophos SafeGuard Disk Encryption 5.50 disponible avec ESDP (Endpoint Security et Data Protection).
- SafeGuard Easy 5.50. À compter de la version 5.50, SafeGuard Easy est le nouveau nom de produit de la solution autonome SafeGuard Enterprise.

Vous pouvez facilement mettre à niveau ces produits vers la suite SafeGuard Enterprise à l'aide de la gestion centralisée afin d'utiliser l'ensemble des fonctions de SafeGuard Enterprise. Pour ce faire, veuillez procéder comme suit :

- Vous devez mettre à niveau SafeGuard Policy Editor vers SafeGuard Management Center.
- Les clients Sophos SafeGuard (autonomes) doivent être mis à niveau vers des clients SafeGuard Enterprise (gérés).

Vous pouvez mettre à niveau SafeGuard Policy Editor vers SafeGuard Management Center afin d'utiliser les fonctions de gestion complètes, par exemple, la gestion des utilisateurs et des ordinateurs, ainsi que la consignation.

17.1 Conditions préalables

- Vous n'avez pas besoin de désinstaller SafeGuard Policy Editor.
- Avant de procéder à la migration, configurez le serveur SafeGuard Enterprise. Pour cela, voir *Configuration du serveur SafeGuard Enterprise* à la page 43.

17.2 Mise à niveau de SafeGuard Policy Editor

Pour la mise à niveau, installez simplement le package SGNManagementCenter.msi sur l'ordinateur sur lequel SafeGuard Policy Editor est configuré.

1. Démarrez SGNManangementCenter.msi à partir du CD du produit.
2. Cliquez sur **Suivant** dans la fenêtre de bienvenue.
3. Acceptez le contrat de licence.
4. Sélectionnez un chemin d'installation.
5. Confirmez la réussite de l'installation.

6. Si nécessaire, redémarrez votre ordinateur.

7. Configurez SafeGuard Management Center. Pour cela, voir *Configuration du serveur SafeGuard Enterprise* à la page 43.

SafeGuard Policy Editor a été mis à niveau vers SafeGuard Management Center.

17.3 Mise à niveau des clients Sophos SafeGuard (autonomes)

Vous pouvez mettre à niveau des ordinateurs dotés d'une configuration autonome Sophos SafeGuard pour en faire des ordinateurs dotés d'une configuration de client SafeGuard Enterprise (géré). Les ordinateurs finaux sont ainsi définis dans SafeGuard Management Center en tant qu'objets pouvant être gérés et disposant d'une connexion avec le serveur SafeGuard Enterprise.

17.3.1 Conditions préalables

- SafeGuard Policy Editor a été migré vers SafeGuard Management Center.
- Vous n'avez pas besoin de désinstaller le logiciel de chiffrement client.
- Veillez à sauvegarder l'ordinateur final avant de procéder à la mise à niveau.
- Vous devez disposer des droits d'administrateur Windows.

17.3.2 Poursuite de la mise à niveau

Pour la mise à niveau, il vous suffit de créer le package de configuration correspondant et de l'attribuer à l'ordinateur :

1. Créez le package de configuration pour le client SafeGuard Enterprise (géré) dans SafeGuard Management Center via **Outils** > **Outil de package de configuration** > **Créer un package de configuration** (**géré**).

2. Attribuez ce package aux ordinateurs correspondants, via une stratégie de groupe.

Avis : lors de la mise à niveau, tous les utilisateurs et tous les certificats sont supprimés et l'authentification au démarrage est désactivée, car l'attribution utilisateur-ordinateur n'est pas mise à niveau. Après la mise à niveau, les ordinateurs finaux ne sont donc plus protégés !

3. Réinitialisez deux fois votre ordinateur après la mise à niveau : la première connexion est toujours effectuée via l'ouverture de session automatique de Windows. De nouvelles clés et de nouveaux certificats sont attribués à l'utilisateur. Par conséquent, il ne peut se connecter à l'authentification au démarrage que lors de la seconde réinitialisation. C'est seulement après la seconde réinitialisation que les ordinateurs finaux sont à nouveau protégés.

L'ordinateur autonome non géré est désormais un ordinateur pouvant être géré de manière centralisée via SafeGuard Enterprise.

18 Mise à niveau de SafeGuard Easy 4.x/Sophos SafeGuard Disk Encryption 4.x vers SafeGuard Enterprise

SafeGuard Easy 4.5x ainsi que Sophos SafeGuard Disk Encryption 4.60 peuvent être directement mis à niveau vers SafeGuard Enterprise 5.50 par la simple installation du package d'installation du client SafeGuard Enterprise sur l'ordinateur.

Le chiffrement des disques durs et des supports amovibles est conservé ; vous n'avez donc pas besoin de les déchiffrer et de les chiffrer à nouveau. Il n'est pas nécessaire non plus de désinstaller SafeGuard Easy ou Sophos SafeGuard Disk Encryption.

Ce chapitre décrit la mise à niveau vers SafeGuard Enterprise, explique les fonctions qui peuvent être migrées et détaille les restrictions.

18.1 Conditions préalables

Les conditions préalables suivantes doivent être remplies :

- La mise à niveau directe a été testée et sa prise en charge est assurée pour SafeGuard Easy 4.5x. Une mise à niveau directe devrait également fonctionner pour les versions entre 4.3x et 4.4x. La mise à niveau directe pour les versions antérieures à 4.3x n'est pas prise en charge. La mise à jour préalable vers SafeGuard Easy 4.50 est nécessaire.
- La mise à niveau directe est prise en charge pour Sophos SafeGuard Disk Encryption version 4.60.
- Windows Installer version 3.01 ou toute version ultérieure doit être installé.
- SafeGuard Easy/Sophos SafeGuard Disk Encryption doit être exécuté sur l'un des systèmes d'exploitation suivants :
  - Windows XP Professionnel Service Pack 2, 3
- Le matériel et les logiciels spécifiques (par exemple le middleware Lenovo ou de clé cryptographique) doivent respecter la configuration minimale requise pour SafeGuard Enterprise.
- La mise à niveau ne peut avoir lieu que si les disques durs sont chiffrés à l'aide des algorithmes suivants : AES128, AES256, 3DES et IDEA.

18.2 Restrictions

La mise à niveau est soumise aux restrictions suivantes :

- Seul le package d'installation du client SafeGuard Device Encryption (SGNClient.msi) avec le jeu de fonctions standard peut être installé. Si SafeGuard Configuration Protection ou SafeGuard Data Exchange doivent être installés en plus, ces installations doivent être effectuées lors d'une autre étape.
- Le package d'installation sans chiffrement basé sur volume (SGNClient_withoutDE.msi) n'est pas pris en charge pour la mise à niveau vers SafeGuard Enterprise.

Les installations suivantes ne peuvent pas être mises à niveau vers SafeGuard Enterprise et l'installation de SafeGuard Enterprise ne doit pas être tentée.

Avis : si vous démarrez une mise à niveau avec les installations suivantes, un message d'erreur (numéro 5006) s'affiche.

  - Installations à double initialisation
  - Installations avec commutateur Compaq actif
  - Installations Lenovo Computrace
  - Disques durs partiellement chiffrés, un secteur d'initialisation chiffré par exemple
  - Disques durs avec des partitions masquées
  - Disques durs chiffrés avec l'un des algorithmes suivants :
    XOR, STEALTH, DES, RIJANDAEL, Blowfish-8, Blowfish-16
  - Scénarios à plusieurs initialisations avec une seconde partition Windows ou Linux

- Les supports amovibles qui ont été chiffrés avec les algorithmes XOR, STEALTH, DES, RIJANDAEL, Blowfish-8 ou Blowfish-16 ne peuvent pas être mis à niveau.

Avis : des données risquent d'être perdues si un périphérique amovible a été chiffré avec l'algorithme XOR, STEALTH, DES, RIJANDAEL, Blowfish-8 ou Blowfish-16 dans SafeGuard Easy. Il est impossible d'accéder aux données du support amovible avec SafeGuard Enterprise après la mise à niveau.

- Les supports amovibles peuvent être convertis dans un format compatible SafeGuard Enterprise. Après la conversion, un support de données chiffré ne peut être lu qu'avec SafeGuard Enterprise et uniquement sur l'ordinateur final ayant servi à sa conversion.
- Les supports amovibles avec des volumes Super Floppy ne peuvent pas être convertis après la migration.

18.3 Fonctionnalités mises à niveau

Le tableau ci-dessous indique les fonctionnalités mises à niveau et leur correspondance dans SafeGuard Enterprise.

SafeGuard Easy/ Sophos SafeGuard Disk Encryption	Mise à niveau	SafeGuard Enterprise
Disques durs chiffrés	Oui	Les clés des disques durs sont protégées par l'authentification au démarrage (POA) de SafeGuard Enterprise. Elles ne sont donc jamais exposées. Si le mode de protection à l'initialisation est sélectionné dans SafeGuard Easy, vous devez désinstaller la version actuelle. L'algorithme de chiffrement du disque dur n'est pas modifié par la mise à niveau. En conséquence, l'algorithme réel de ce type de disque dur mis à niveau peut différer de la stratégie générale de SafeGuard Enterprise.
Supports amovibles chiffrés (ne concerne pas Sophos SafeGuard Disk Encryption)	Oui	Les supports de données, par exemple les cartes mémoire USB, peuvent être convertis dans un format compatible SafeGuard Enterprise. **Avis :** après la conversion, un support de données chiffré ne peut être lu qu'avec SafeGuard Enterprise et uniquement sur l'ordinateur final ayant servi à sa conversion. La conversion doit être confirmée cas par cas. Pour plus d'informations sur les exceptions, voir *Restrictions* à la page 120.
Algorithmes de chiffrement	Dans une certaine mesure	Les algorithmes AES128, AES256, 3DES et IDEA peuvent être migrés. AES-128 et 3-DES ne peuvent néanmoins pas être sélectionnés dans SafeGuard Management Center pour les supports à chiffrer. Pour plus d'informations sur les algorithmes qui ne peuvent pas être migrés, voir *Restrictions* à la page 120.
Challenge/Réponse	Dans une certaine mesure	La procédure challenge/réponse est conservée.

SafeGuard Easy/ Sophos SafeGuard Disk Encryption	Mise à niveau	SafeGuard Enterprise
Noms d'utilisateur	Non	Étant donné que les noms d'utilisateur Windows sont utilisés dans SafeGuard Enterprise, vous n'avez pas besoin de réutiliser les noms d'utilisateur SafeGuard Easy/Sophos SafeGuard Disk Encryption spécifiques. Pour enregistrer les ordinateurs mis à niveau, vous procédez donc de la même façon qu'avec une nouvelle installation de SafeGuard Enterprise : en attribuant de façon centralisée ou en enregistrant localement les utilisateurs de l'ordinateur.
Mots de passe utilisateur	Non	Étant donné que les mots de passe Windows sont utilisés dans SafeGuard Enterprise, vous n'avez pas besoin de réutiliser les mots de passe SafeGuard Easy/Sophos SafeGuard Disk Encryption spécifiques. Les mots de passe SafeGuard Easy/ Sophos SafeGuard Disk Encryption ne seront ainsi pas mis à niveau.
Stratégies, paramètres (par exemple, longueur minimum de mot de passe)	Non	Pour garantir la cohérence de tous les paramètres, aucune mise à niveau automatique n'est exécutée. Les stratégies doivent être redéfinies dans SafeGuard Management Center.
Authentification de préinitialisation	Non	L'authentification de préinitialisation (PBA) est remplacée par l'authentification au démarrage (POA) de SafeGuard Enterprise.
Installations sans GINA	Oui	Les installations sans GINA sont mises à niveau vers SafeGuard Enterprise avec SGNGINA.

SafeGuard Easy/ Sophos SafeGuard Disk Encryption	Mise à niveau	SafeGuard Enterprise
Clés cryptographiques/ Cartes à puce (ne concerne pas Sophos SafeGuard Disk Encryption)	Dans une certaine mesure	Vous pouvez continuer à utiliser les clés cryptographiques/cartes à puce dans SafeGuard Enterprise. Néanmoins, les informations d'identification ne sont pas mises à niveau. Les clés cryptographiques utilisées dans SafeGuard Easy doivent donc être redélivrées dans SafeGuard Enterprise et, comme pour tout autre ordinateur final SafeGuard Enterprise, configurées à l'aide de stratégies. Les informations d'identification SafeGuard Easy, regroupées sous forme de fichier sur les clés cryptographiques/cartes à puce, restent telles quelles, mais ne peuvent être utilisées pour que la connexion aux ordinateurs prenant en charge SafeGuard Easy. Le cas échéant, le middleware de clé cryptographique/carte à puce utilisé doit être mis à jour vers une version prise en charge par SafeGuard Enterprise.
Connexion avec le lecteur d'empreintes digitales Lenovo	Dans une certaine mesure	La connexion par empreintes digitales peut toujours être utilisée dans SafeGuard Enterprise. Le matériel et le logiciel du lecteur d'empreintes digitales doivent être pris en charge par SafeGuard Enterprise et les données utilisateur d'empreintes digitales doivent être de nouveau déployées. Pour plus d'informations sur la connexion par empreintes digitales, consultez l'aide de l'utilisateur.

18.4 Préparation pour la mise à niveau

Vous devez prendre les mesures suivantes avant de démarrer l'installation de SafeGuard Enterprise :

- Avant la mise à niveau des ordinateurs finaux, préparez un package de configuration SafeGuard Enterprise à l'aide de SafeGuard Management Center. Après l'installation du logiciel de chiffrement SafeGuard Enterprise sur les ordinateurs finaux, déployez-y le package de configuration. Les stratégies transférées avec le premier package de configuration doivent correspondre à la configuration précédente de l'ordinateur SafeGuard Easy/Sophos SafeGuard Disk Encryption.

  Si aucun package de configuration n'est installé avec la mise à niveau, tous les lecteurs chiffrés avec SafeGuard Easy/Sophos SafeGuard Disk Encryption restent chiffrés.

- Pour des raisons de sécurité, créez une sauvegarde complète des ordinateurs que vous mettez à niveau.

- Effectuez les étapes recommandées avant l'installation de SafeGuard Enterprise, par exemple l'utilisation des commandes « chkdsk » et « defrag ».

  Pour plus d'informations sur les commandes « chkdsk » et « defrag », consultez notre base de connaissances (en anglais) :

  chdsk : *http://www.sophos.com/support/knowledgebase/article/107799.html*

  defrag : *http://www.sophos.com/support/knowledgebase/article/109226.html*

- Créez une sauvegarde du noyau valide et enregistrez-la sur un emplacement toujours accessible (par exemple, un chemin d'accès au réseau). Pour plus d'informations, consultez les manuels et l'aide de SafeGuard Easy 4.5x/Sophos SafeGuard Disk Encryption 4.60, et plus précisément le chapitre *Saving the system kernel and creating emergency media* (Enregistrement du noyau du système et création de supports d'urgence).

- Pour des raisons de sécurité, créez un environnement de test pour la première mise à niveau.

- Lorsque vous procédez à une mise à niveau depuis des versions plus anciennes de SafeGuard Easy, effectuez tout d'abord une mise à niveau vers la version 4.50.

- Laissez les ordinateurs sous tension durant tout le processus de mise à niveau.

- Le responsable de la sécurité doit conserver les informations d'identification Windows des utilisateurs au cas où ces utilisateurs perdraient leur mot de passe Windows après la migration. Cela peut se produire si les utilisateurs se sont connectés auparavant via l'authentification de préinitialisation et se connectent ensuite via la connexion sécurisée Windows. Les utilisateurs n'utilisent donc jamais leurs informations d'identification Windows.

Avis : les utilisateurs doivent connaître leur mot de passe de connexion à Windows avant la mise à niveau. Cette étape est essentielle, car il est impossible de définir un mot de passe Windows après mise à niveau et installation de SafeGuard Enterprise. Si les utilisateurs ne connaissent pas leur mot de passe Windows car ils ont utilisé la connexion automatique sécurisée de SafeGuard Easy/ Sophos SafeGuard Disk Encryption, ils ne pourront pas se connecter à SafeGuard Enterprise puisque la connexion automatique vers Windows sera refusée. Il existe donc un risque de perte de données car les utilisateurs ne peuvent plus accéder à leurs ordinateurs.

18.5 Lancement de la mise à niveau

L'installation peut être effectuée sur un système SafeGuard Easy/Sophos SafeGuard Disk Encryption en cours d'exécution. Aucun déchiffrement de disques durs ou de volumes chiffrés n'est nécessaire.

Utilisez le package du client SafeGuard Device Encryption (SGNClient.msi) situé dans le dossier du produit avec le jeu de fonctions standard. Vous ne pouvez pas utiliser le package client SGNClient_withoutDE.msi.

Avis : pour une mise à niveau réussie, l'installation doit être exécutée de manière centralisée, en mode sans surveillance. L'installation via le dossier de configuration n'est pas recommandée.

Procédez comme suit :

1. Double-cliquez sur WIZLDR.exe dans le dossier du programme SafeGuard Easy/Sophos SafeGuard Disk Encryption présent sur l'ordinateur final à mettre à niveau : cette opération démarre l'assistant de migration.

2. Dans l'assistant de migration, saisissez le mot de passe système et confirmez en choisissant **Suivant**. Dans **Dossier de destination**, confirmez la valeur par défaut en choisissant **Suivant** et cliquez sur **Terminer** pour terminer l'action. Un fichier de configuration de migration, `SGEMIG.cfg`, est créé.

3. Dans l'Explorateur Windows, changez le nom du fichier `SGEMIG.cfg` en `SGE2SGN.cfg`. Conservez-le à un endroit accessible pour l'ordinateur pendant la mise à niveau.

Avis : des droits de propriété/création doivent être définis pour ce fichier et son chemin d'accès de stockage pendant la mise à niveau. Dans le cas contraire, la mise à niveau peut échouer et un message indiquant que le fichier `SGE2SGN.cfg` est introuvable peut s'afficher.

4. Entrez la commande « msiexec » dans l'invite de commande pour installer le package de préinstallation de SafeGuard Enterprise ainsi que le package d'installation du client sur l'ordinateur final SafeGuard Easy/Sophos SafeGuard Disk Encryption. Ajoutez le paramètre MIGFILE indiquant le chemin d'accès au fichier de configuration de migration `SGE2SGN.cfg` :

EXEMPLE :

```
msiexec /i
\\Distributionserver\Software\Sophos\SafeGuard\SGxClientPreinstall.msi
msiexec /i \\Distributionserver\Software\Sophos\SafeGuard\SGNClient.msi
/L*VX \\Distributionserver\Software\Sophos\SafeGuard\%Computername%.log“

MIGFILE=\\Distributionserver\Software\Sophos\SafeGuard\SGE2SGN.cfg
```

Une fois la mise à niveau correctement effectuée, SafeGuard Enterprise peut être utilisé sur l'ordinateur.

En cas d'échec de la mise à niveau, SafeGuard Enterprise/Sophos SafeGuard Disk Encryption peut tout de même être utilisé sur l'ordinateur. Le cas échéant, SafeGuard Enterprise est automatiquement supprimé.

18.6 Configuration des ordinateurs finaux mis à niveau

Les ordinateurs finaux sont initialement configurés par les packages de configuration qui, entre autres choses, définissent si l'ordinateur est autonome ou géré de manière centralisée et activent l'authentification au démarrage.

Ainsi, pendant la mise à niveau, vous devez installer tout d'abord le package de préinstallation, puis SGNClient.msi. Ce n'est qu'après que l'authentification au démarrage a été activée et que l'utilisateur s'est correctement connecté à Windows que la configuration de l'ordinateur final doit avoir lieu.

1. Créez le package de configuration initial dans SafeGuard Management Center via **Outils** > **Outil de package de configuration** avec les paramètres de stratégie requis.

2. Installez le package de configuration sur les ordinateurs finaux.

Avis : les stratégies transférées avec le premier package de configuration SafeGuard Enterprise doivent correspondre à la configuration précédente de l'ordinateur SafeGuard Easy/Sophos SafeGuard Disk Encryption.

18.7 Après la mise à niveau

Après une mise à niveau réussie, les éléments suivants sont disponibles dans SafeGuard Enterprise après la connexion à l'authentification au démarrage :

- les clés et algorithmes des volumes chiffrés ;
- les clés et les algorithmes des supports amovibles chiffrés (concerne uniquement la mise à niveau depuis SafeGuard Easy).

Les volumes chiffrés restent inchangés et les clés de chiffrement sont automatiquement converties dans un format compatible avec SafeGuard Enterprise.

Avis : pour déchiffrer le disque dur ou ajouter et supprimer des clés de chiffrement du disque dur, l'utilisateur doit tout d'abord redémarrer l'ordinateur.

Les stratégies doivent être réinitialisées par SafeGuard Management Center pour correspondre à la configuration précédente de l'ordinateur SafeGuard Easy/Sophos SafeGuard Disk Encryption.

Migration du support amovible

Avis : la migration des supports amovibles ne concerne pas Sophos SafeGuard Disk Encryption.

Le support amovible chiffré reste inchangé également, mais les clés doivent être converties dans un format compatible avec SafeGuard Enterprise.

Avis : ainsi, après la conversion, un support de données chiffré ne peut être lu qu'avec SafeGuard Enterprise et uniquement sur l'ordinateur final ayant servi à sa conversion pendant la migration.

Pour déchiffrer le support amovible ou ajouter et supprimer des clés de chiffrement du disque dur, l'utilisateur doit d'abord retirer le support de l'ordinateur, puis le réinsérer.

Lorsque vous accédez à un support amovible après migration, l'utilisateur doit confirmer explicitement la conversion des clés de chiffrement dans un format compatible avec SafeGuard Enterprise. La stratégie appropriée de chiffrement basé sur volume doit être présente sur l'ordinateur final avant la conversion, faute de quoi les clés ne sont pas converties.

L'utilisateur est invité à confirmer la conversion pour chaque support amovible. Un message approprié s'affiche.

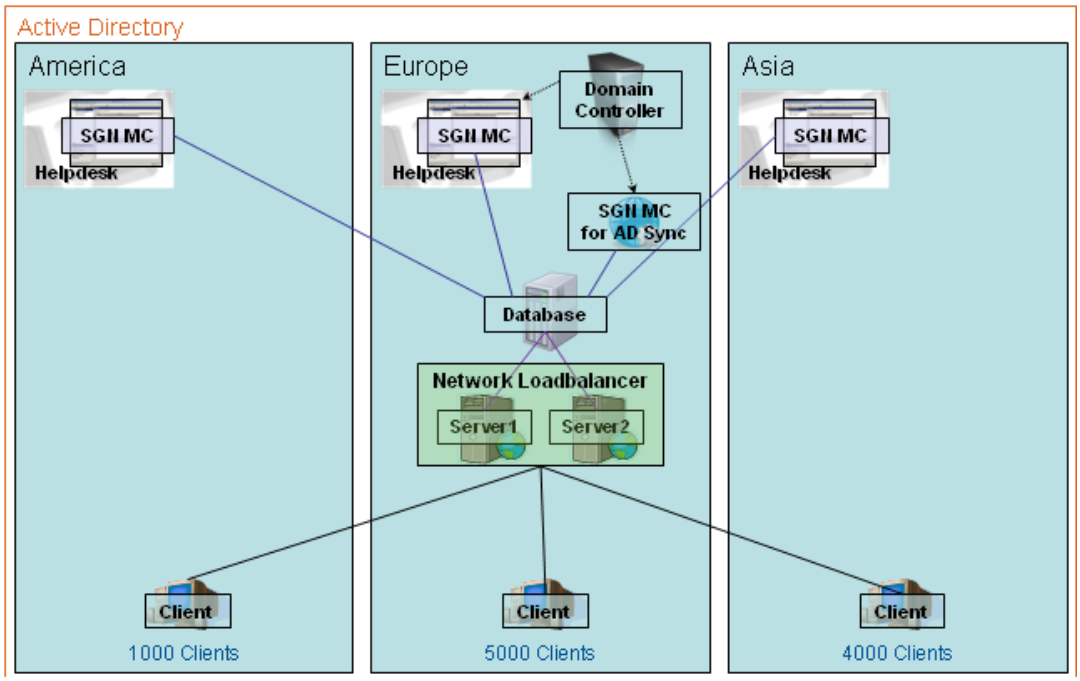
- Si l'utilisateur confirme la conversion, il bénéficie d'un accès complet aux données migrées.
- Si l'utilisateur refuse la conversion, les données migrées peuvent tout de même être lues et modifiées.

Les supports amovibles récemment ajoutés sont chiffrés, comme sur tout client SafeGuard Enterprise, si la stratégie appropriée est présente sur le point de terminaison.

19 Mise à jour du système d'exploitation

Une fois SafeGuard Enterprise installé, il est uniquement possible de mettre à jour la version du Service Pack du système d'exploitation installé. Par exemple, vous pouvez installer une mise à jour de Service Pack Windows XP. Vous ne pouvez cependant pas migrer d'un système d'exploitation à un autre lorsque SafeGuard Enterprise est installé : par exemple, vous ne pouvez pas migrer de Windows XP vers Windows Vista lorsque SafeGuard Enterprise est installé.

20 Annexe : Scénario de pratique recommandée



Dans ce scénario, l'Europe est le lieu idéal pour la base de données SafeGuard Enterprise. Les raisons suivantes sont invoquées :

- Le service Active Directory est situé en Europe et permet donc d'exécuter une synchronisation rapide.
- La gestion centralisée à l'aide de SafeGuard Management Center est effectuée en Europe.
- Le serveur IIS se trouve en Europe.
- La plupart des utilisateurs se trouvent en Europe.

21 Support technique

Vous pouvez obtenir du support technique pour les produits Sophos de l'une des manières suivantes :

- Visitez le forum SophosTalk à l'adresse http://community.sophos.com/ et recherchez d'autres utilisateurs qui connaissent le même problème.
- Visitez la base de connaissances du support technique de Sophos à l'adresse http://www.sophos.fr/support/
- Téléchargez la documentation des produits à l'adresse http://www.sophos.fr/support/docs/
- Envoyez un courriel à support@sophos.com, y compris le(s) numéro(s) de version du ou des logiciels Sophos, le(s) système(s) d'exploitation et le(s) niveau(x) de correctif ainsi que le texte de tout message d'erreur.

22 Copyright

Copyright © 1996 - 2010 Sophos Group et Utimaco Safeware AG. Tous droits réservés.

Aucune partie de cette publication ne peut être reproduite, stockée dans un système de recherche documentaire ou transmise, sous quelque forme ou par quelque moyen que ce soit, électronique, mécanique, photocopie, enregistrement ou autre sauf si vous possédez une licence valide, auquel cas vous pouvez reproduire la documentation conformément aux termes de cette licence ou si vous avez le consentement préalable écrit du propriétaire du copyright.

Sophos est une marque déposée de Sophos Plc et de Sophos Group. SafeGuard est une marque déposée de Utimaco Safeware AG - a member of the Sophos Group. Tous les autres noms de produits et d'entreprises cités dans ce document sont des marques ou des marques déposées de leurs propriétaires respectifs.

Tous les produits SafeGuard sont sous le copyright d'Utimaco Safeware AG- a member of the Sophos Group, ou, le cas échéant, des concédants de la licence. Tous les autres produits Sophos sont sous copyright de Sophos Plc, ou, le cas échéant, des concédants de la licence.

Vous trouverez des informations de copyright des fournisseurs tiers dans le fichier Disclaimer and Copyright for 3rd Party Software.rtf de votre répertoire d'installation.